Cybersikkerhet i måleverdikjeden for fjellskredvarsling

Masterstudium i teknisk samfunnssikkerhet

Universitet i Stavanger

Juni 2020

Mari Aarland

Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i teknisk samfunnssikkerhet	Vårsemesteret, 2020 Åpen
Forfatter: Mari Aarland	Mari Aarland (signatur forfatter)
Fagansvarlig: Sissel H. Jore **Veileder**: Janne M. Hagen	
Tittel på masteroppgaven: Cybersikkerhet i måleverdikjeden for fjellskredvarsling **Engelsk tittel**: Cybersecurity in Meetering Value Chain on Mountain Landslide Warning	
Studiepoeng: 30	
Emneord: Cybersikkerhet, digitalisering, digital verdikjede, fjellskredvarsling, rammeverk, Resilience Engingeering, risikoanalyse, risikostyring, sikkerhetskultur og skyløsning	**Sidetall**: 79 + vedlegg/annet: 120 Skien, 15.06.2020

Forside for masteroppgave
Det teknisk-naturvitenskapelige fakultet

FORORD

Masteroppgaven er skrevet som siste del av studiet teknisk samfunnssikkerhet ved Universitet i Stavanger. Arbeidsprosessen har vart fra desember 2019 til juni 2020.

Jeg ønsker å takke alle informantene som har bidratt til oppgaven min med et stort engasjement, og til spennende diskusjoner om et krevende tema. Takk for at dere har vært åpne og delt deres erfaringer med meg slik at oppgaven ble gjennomførbar.

Tusen takk til veileder Janne Hagen for at du ga meg en så spennende oppgave, men også for den oppfølgningen du har gitt meg. Dine råd har gjort at jeg har holdt motivasjonen oppe til tross for noen tøffe perioder med mye frustrasjon.

Takk også til fagansvarlig Sissel Jore for gode innspill. Takk til seksjonsleder Arne Bjørn for gode bidrag til oppgaven.

Jeg ønsker også å rette en stor takk til min søster Siri, som til det utrettelige har måttet høre på alle mine tanker. Takk for at du stiller opp når jeg har hatt behov for det, for at du har lest gjennom oppgaven kanskje like mange ganger som meg selv, og for alle rådene du kommer med – din hjelp har vært uvurderlig.

Til slutt ønsker jeg også å takke Martin, som til tross for at temaet ikke er hans favoritt, har hørt på mens jeg har lest opp kapittel for kapittel. Han har støttet meg underveis og vært der for meg når perioder har vært tunge og slitsomme. Takk for at du holder ut med en emosjonell og utbrent masterstudent.

Skien, 15.juni.2020

Mari Aarland

SAMMENDRAG

Digitaliseringsprosessen som Norges vassdrag- og energidirektorat (NVE) nå ønsker å iverksette skal forbedre dagens teknologibruk. Ved hjelp av digitale målere og skyløsning kan NVE gjøre data mer tilgjengelig, effektivisere arbeidsoppgaver, gi bedre beslutningsgrunnlag og samvirke bedre. NVE er avhengig av digitale verdikjeder som strekker seg over flere sektorer. Den største sårbarheten er som Nasjonal Sikkerhetsmyndighet (NSM) sier, kompleksiteten i det norske digitale samfunnet, og ved implementering av komplekse digitale løsninger kommer det flere sårbarheter.

Studiens problemstilling er følgende: *Hvordan kan NVE sikre den digitale og skybaserte måleverdikjeden for fjellskredvarsling?* Formålet til studien har vært å undersøke hvordan man ivaretar cybersikkerheten i digitale målere og skyløsningen Azure i måleverdikjeden for fjellskredvarsling hos NVE.

Studiens undersøkelse har en kvalitativ tilnærming hvor metodene dokumentanalyse og intervju blir sammenstilt i en risikoanalyse. Risikoanalysen benyttet i studiet baserer seg på metodikken fra ISO 31000. Analysen tar for seg tre ulike verdikjeder: intern, norsk leverandør og transnasjonal leverandør. Datainnsamlingen har bestått av relevante dokumenter og åtte intervjuer av nøkkelpersoner innenfor studiets problemstilling. Det teoretiske kapittelet bidrar med begrepsforklaring av cybersikkerhet, sikkerhetskultur og risiko knyttet til sårbarhet, trussel og verdi.

Resultater fra risikoanalysen viser at det er størst risiko knyttet til tap av måledata. Dagens måleinfrastruktur er utrustet med gode tekniske barrierer for å sikre redundans. Risikoen ligger derimot på den stadig mer komplekse og uoversiktlige verdikjeden, hvor man ikke har tilstrekkelig med kontroll på leverandører. Samtidig blir det avdekt manglende gode rutiner for en tverrsektoriell risiko. Menneskelige feilhandlinger som verdivurdering av skjermingsverdig informasjon og mangelfulle risikovurderinger er fremhevet ved flere anledninger. Disse feilhandlingene er potensielle sårbarheter som kan føre til integritets- og konfidensialitetsbrudd.

Studien konkluderer med at risikoen er betydelig høyrere for de eksterne verdikjedene grunnet manglende mulighet for kontroll. Konklusjonen avslutter med anbefalte tekniske og organisatoriske sikringstiltak: segregerte nettverk, logging av aktivitet, minimere administratorrettigheter, skaffe oversikt over alle åpne porter (brannmur, ruter, svitsjer), gjennomføre inntrengingstester, ende-til-ende kryptering, overordnet rammeverk for cybersikkerhet med tilhørende anbefalte aktiviteter.

INNHOLDSFORTEGNELSE

Tabeller:

Figurer:

Forkortelser

ADSL/DSL: Asymmetrisk digital abonnentlinje

DSB: Direktorater for samfunnssikkerhet og beredskap

DMZ: Demilitarisert sone

IKT: Informasjons- og kommunikasjonsteknologi

GB-InSAR: Bakkebasert satellittmåling

IDS: Intrusion Detection System

ISO: International Organization for Standardization

IT: Informasjonsteknologi

IIoT: Industrial Internet of Things

NOU: Norges offentlige utredning

NGU: Norges geologiske undersøkelse

NSM: Nasjonal sikkerhetsmyndighet

NVE: Norges vassdrag- og energidirektorat

SB-InSAR: Satellittbasert radarmåling

SVF: Seksjon for fjellskredvarsling

1 KAPITTEL: INNLEDNING

1.1 TEMATIKK FOR STUDIET

Dagens samfunn står overfor et paradigmeskift innen digitalisering, som skaper både muligheter og utfordringer. Det er i stor grad basert på et økende utviklingsbehov hos ulike interessenter[1]. For å imøtekomme endringsbehovet og krav fra interessenter, eksempelvis regjeringens digitaliseringsstrategi, har Norges vassdrag- og energidirektorat (NVE heretter) behov for å ta i bruk ny teknologi og utvikle supplerende digitale løsninger.
En av NVE sine ansvarsoppgaver er å beskytte kritisk infrastruktur. NVE har også ansvaret for å overvåke faren for skred/flom, og fungerer som opplysningsorgan for befolkningen for å forhindre tap av liv, helse og andre materielle verdier. De er også beredskapsmyndighet for energiforsyningen, dette innebærer å føre tilsyn med sikkerhet og beredskap.

Ifølge NOU 2006:6 blir en kritisk infrastruktur definert som «*de anlegg og systemer som er helt nødvendige for å opprettholde samfunnskritiske funksjoner som dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse*» [1, p. 16]. NVE har blant annet ansvaret for å overvåke tilstanden til fjellet «Mannen», et ustabilt fjellparti lokalisert i Rauma kommune. NVE anvender måleinfrastrukturen sin på å kartlegge bevegelser i fjellet som de siste årene har vært på et svært aktivt nivå. Konsekvensene av ras er estimert til at det kan ramme 1650 innbyggere bosatt i Romsdalen med en tsunami som resultat [2].

Digitaliseringen åpner opp for muligheter hos NVE til å kunne benytte blant annet Industrial Internet of Things (IIoT) i større grad [3]. IIoT er en samlebetegnelse for fysiske enheter brukt i industrien som er koblet sammen i et nettverk, og som kommuniserer med hverandre via internett [4]. I 2020 forventes det et operativt femte generasjons mobilnett (5G) som skal øke hastigheten ytterligere. 5G-nettet er 10-100 ganger raskere enn 4G med enda høyere kapasitet, noe som gir større muligheter for å øke generering av data ved bruk av digitale målere [5].

1.2 NVES DIGITALE MÅLERE OG BRUK AV SKYLØSNING

Denne studien vil ta for seg IIoT i form av digitale målere og bruken av disse i en skybasert løsning. Å koble opp digitale målere til internett vil kunne gi bedre informasjonsgrunnlag som ikke tidligere har vært tilgjengelig. Informasjon som kan være med på å forutse uønskede

[1] *Interessenter kan forstås som kunder, brukere, leverandører, organisasjoner og myndigheter*

hendelser eller feil som kan oppstå. Digitale målere vil kunne skape mer forutsigbarhet for NVE, og kan blant annet forbedre sanntidsovervåkningen, forbedre hastigheten til informasjonsdelingen, overvåke vedlikeholdsbehov og sikkerheten på de digitale målerne. Et ønske om å forbedre målesystemene med nye digitale løsninger er også i tråd med de politiske føringene for digitaliseringen i Norge.

Digitaliseringen åpner ikke bare opp for ny teknologibruk for NVE, men også tilgjengeliggjøring og analyse av data. Overgangen fra lokal lagring av data til en skybasert løsning vil også være en del av digitaliseringsprosessen NVE nå står overfor. Microsoft Azure er en skyløsning som NVE ønsker å benytte til å lagre sine data for å gjøre de mer tilgjengelig. NVE er pålagt å publisere og distribuere data i henhold til Norsk lisens for offentlig data (NLOD), dette gjelder samfunnsnyttig informasjon som gjerne kommer i form av åpne datasett som kan benyttes av andre aktører. Skyløsningen kan hjelpe NVE med å anvende historisk data i kombinasjon med sanntidsdata for å kunne predikere om fremtidige hendelser. Med tilgjengeliggjøring av predikasjoner fra NVE kan man også se disse i en større kontekst hvor man kan kjøre simuleringer og sammenstille analyser fra ulike datakilder [3].

På samme måte som digitaliseringen åpner opp for nye muligheter, åpner det også opp for flere digitale angrep hvor NVE er et attraktivt mål for potensielle trusselaktører. Årlig gis det ut fire trussel- og risikovurderinger av samfunnet fra Nasjonal sikkerhetsmyndighet (NSM), Direktoratet for samfunnssikkerhet og beredskap (DSB), Etterretningstjenesten (E-tjenesten) og Politiets sikkerhetstjeneste (PST), hvorav angrep mot kritisk infrastruktur blir nevnt i samtlige av rapportene[2]. Selv om digitaliseringen åpner opp for nye trusler, vil det også by på utfordringer om NVE blir en digital sinke. Dette skaper et paradoks da det vil skape sårbarheter uansett om man velger å implementere ny teknologi eller om man velger å fortsette som før. Bruk av gammel teknologi medfører også utfordringer og kan være lettere for trusselaktørene å komme gjennom basert på tidligere angrep, ved implementering av ny teknologi skaper man potensielt nye veier inn for trusselaktørene som man ikke har avdekt før. Det vil være essensielt at NVE har gode sikkerhetskrav til leverandørene sine og at de selv setter fokus på å sikre informasjonssystemene sine. Den kritiske infrastrukturen som NVE har ansvar for er en av bærebjelkene i samfunnet, derfor er det kritisk at denne infrastrukturen er intakt til enhver tid [6].

[2] NOU 2018:14 (2018) *Tap/forstyrrelser i funksjonaliteten kan få alvorlige konsekvenser for offentlig sektor*

Studien vil følgende være en analytisk tilnærming for å utforske hvilke sårbarheter NVE står ovenfor ved å implementere nye digitale målere og bruk av skyløsning i måleverdikjeden for skredvarsling. I studiet vil ny teknologi for NVE være en betegnelse på digitale målere anvendt i skredvarslingen, og Microsoft Azure som skyløsning. Gjennom en risikoanalyse skal det kartlegges hvor sårbarheten ligger, og avdekke hvordan dette vil påvirke den digitale verdikjeden.

Cybersikkerhet – Konseptualisering
Informasjonssikkerhet, IKT-sikkerhet, datasikkerhet, IT-sikkerhet, cybersikkerhet. Fellesnevneres for begrepene er sikkerhet og det handler om å sikre informasjonsverdiene våre. Men begrepene tar for seg ulike dimensjoner rundt sikkerhet knyttet til vår åndsrett, hvor cybersikkerhet er et begrep brukt for å beskrive beskyttelsen mot tilsiktede handlinger som kan være sårbare via IKT. En mangel i begrepet er at det ikke innebærer den tilsiktede delen som er en stor årsaksfaktor til sikkerhetsbrudd. I begrepet ligger det også det å beskytte nettverk, programmer og systemer fra digitale angrep, hvor formålet til angrepet kan være det å få tilgang, ødelegge, kompromittere, tilegne seg økonomisk gevinst eller forstyrre signalsendingen for å hindre viktig informasjon i å bli distribuert **[7]**.

Tabell 1.2.1 Tekstboks om cybersikkerhet

1.3 PROBLEMSTILLING

Studiet skal som nevnt ta for seg utfordringene som skjer ved implementering av ny teknologi i den kritiske infrastrukturen til NVE, og vil mer spesifikt ta for seg digitale målere i skredvarsling og bruk av den skybaserte plattformen Microsoft Azure. Det vil ikke være noe løsning på hvordan NVE skal håndtere paradigmeskiftet inn mot en digitalisert hverdag, men fungere som en veileder til hvordan vurdere cybersikkerhetens tilstand ved implementering av ny teknologi. Fokuset i studiet vil hovedsakelig være på prosessen for hvordan en slik risikovurdering kan gjennomføres av NVE, dette vil bli belyst med følgende problemstilling:

Hvordan kan NVE sikre den digitale og skybaserte måleverdikjeden for fjellskredvarsling?

Som et supplement til problemstilling er det også utarbeidet tre forskningsspørsmål som skal bidrar til å adressere og avdekke underbyggende faktorer som påvirker hvordan studiet svarer ut problemstillingen.

Forskningsspørsmål:

i. Hvordan ser risikobildet ut for måleverdikjeden skredvarsling, og hva er den største risikoen?

ii. Hvordan kan en styrke evnen til å beskytte seg mot ytre påkjenninger i den digitale måleverdikjeden?
iii. Hvilken risikometodikk er best skikket til å redusere sårbarheten, samt bevare integriteten og tilgjengeligheten av data ved bruk av digitale målere og skybasert løsning?

Problemstillingen samt forskningsspørsmålene skal bli besvart ved å kartlegge den digitale verdikjeden til NVE for å ivareta sikker forankring av nye digitale målere og skyløsning. Funn fra dokumentanalysen og utvalgte informanter med ekspertkunnskap skal fremstilles i en risikoanalyse og skal tilsammen forme resultater om sikkerhetstilstanden i den digitale og skybaserte måleverdikjeden for fjellskredvarsling hos NVE.

Avgrensninger

Digitalisering er et omfattende begrep, men i dette studiet vil det kun omhandle nye digitale målere og skyløsningen Azure. Hovedfokuset er rettet mot cybersikkerhet og vil derfor ikke gå i dybden på teknologien. Kundeopplevelse blir nevnt i en bisetning fordi NVE har et ansvar ovenfor sine brukere av systemet, men hvorvidt disse blir innfridd ved ny implementert teknologi vil ikke bli utforsket. Studiet vil heller ikke ta stilling til økonomiske eller miljømessige konsekvenser eller andre behov for implementering av teknologi. Studiet vil i noe grad gå inn på organisatoriske og kompetansehevende tiltak, men dette vil kun være supplerende i forhold til sikkerhet og risikovurderingene som vil være hovedfokuset.

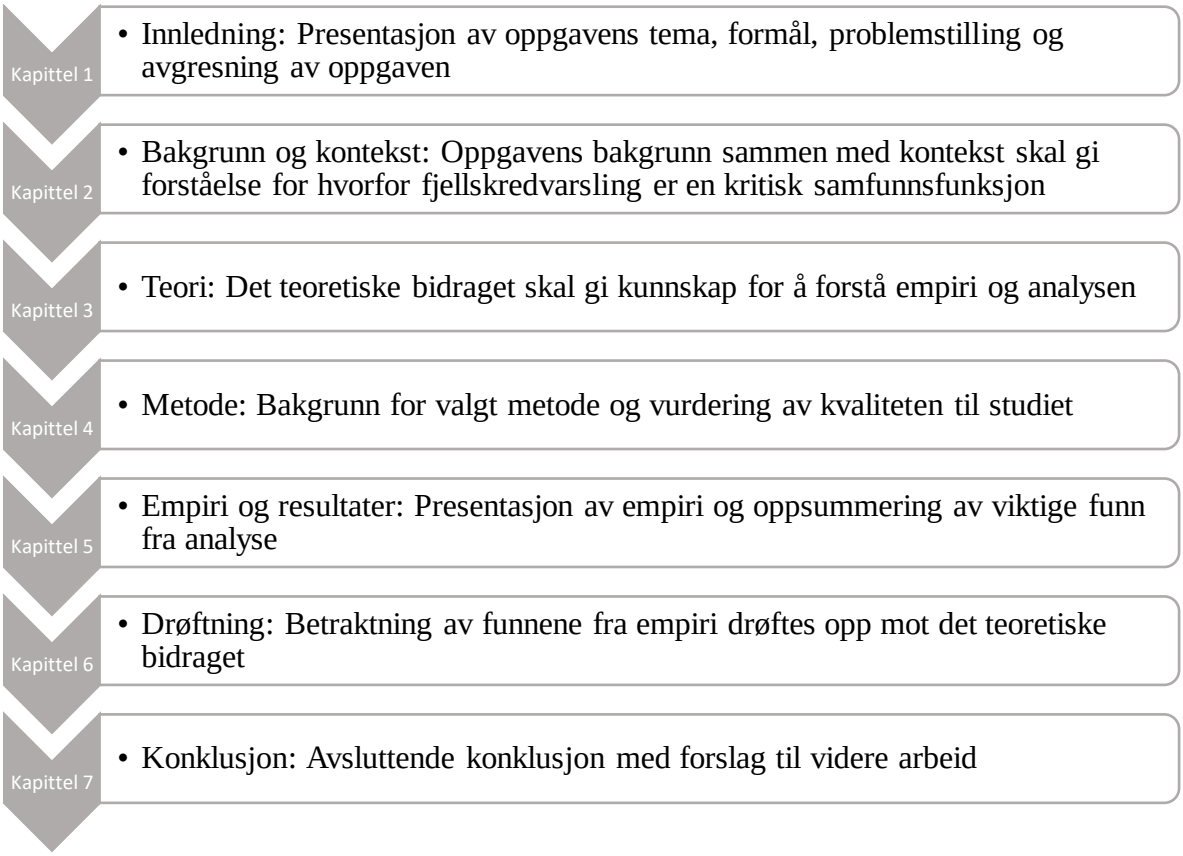
NVE har ansvar for flere samfunnsoppgaver, men i dette studiet vil det kun være fokus på deres ansvar innenfor fjellskredvarsling. Dette utelukker med andre ord løsmasseskred, snøskred, flomvarsel og sentral-, regional- og distribusjonsnettet av vannkraftverk som også er en del av NVEs ansvarsoppgaver.

NVE sin måleverdikjede for skredvarsling er sammensatt av mange ulike aktører. Det ville vært for omfattende å ta for seg cybersikkerheten for hele måleverdikjeden for fjellskredvarsling. For at studiet skal være gjennomførbart er det derfor valgt å fokusere på deler av verdikjeden for den kritiske samfunnsfunksjonen skredvarsling. Bakgrunnen for dette er fordi måleverdikjeden er transnasjonal. Måleverdikjeden ligger også under flere jurisdiksjoner som påvirker håndteringen av cybersikkerheten. Derfor vil de regulatoriske rammeverkene ikke bli belyst annet enn overvåkingssenterets krav fra TEK 17. Videre avgrenses studiet til å ekskludere leverandører for måleverdikjeden som ikke er en del av

NVE. Dette er på bakgrunn av omfanget til analysen som ikke ville vært gjennomførbar i tidsrommet gitt for dette studiet. Det vil heller ikke være en sammenstilling for hvordan risikoen ser ut for NVE nå, men hvordan det blir ved implementering av ny teknologi før og etter sikringstiltak.

1.4 STUDIETS STRUKTUR

Studiets struktur er lagt opp slik at leseren får best mulig utgangspunkt for å forstå det gjennomgående temaet i studiet.



2 KAPITTEL: BAKGRUNN OG KONTEKST

NVE er et direktorat underlagt olje- og energidepartementet (OED) som har ansvaret for å forvalte Norges vann- og energiressurser, samt ivareta de statlige forvaltningsoppgavene innenfor skredforebygging. Ut ifra risikoklassifiseringen fra Norges geologiske undersøkelse (NGU) skal NVE prioritere hvilke fjellparti som er aktuelle for overvåkning. NVE har også ansvaret for å forvalte midler til sikringstiltak for eksisterende bebyggelse, hvorav et av sikringstiltakene er overvåking av ustabile fjellparti. Den operative overvåkningen har NVE ansvar for, hvor de til enhver tid skal fastsette et farenivå for fjellpartiene som overvåkes. Dersom det skjer en endring av farenivå skal NVE varsle beredskapsaktørene, og NVE skal

bistå med informasjon om fjellets utvikling til lokale og regionale beredskapsaktører ved en fjellskredhendelse [8].

Måleinfrastrukturen for fjellskredvarsling sender ut informasjon daglig med oppdateringer om tilstanden til de ustabile fjellpartiene [9]. Det er essensielt at disse målerne til enhver tid fungerer og har minimalt med nedetid for å ha et så korrekt bilde av tilstanden i det tidsrommet. Måleinfrastrukturen er en viktig del av verdikjeden til NVE for å kunne opprettholde sitt samfunnsansvar. Det er nå et ønske/mål om å implementere digitale målere i måleinfrastrukturen og skybasert løsning som forbedrer tilgjengeligheten og bevare integriteten til informasjonsutvekslingen. Dette krever en grundig risikovurdering av eventuelle sårbarheter som oppstår ved overgangen til digitale målere. I tillegg skal informasjon sendes over til den skybaserte løsningen Microsoft Azure.

Microsoft Azure er en tjeneste for databehandling i skyen, hvor det er muligheter for å lagre data eller kjøre ulike programvarer. Informasjonen lagres blant millioner av servere som er lokalisert på en sikker plass i de ulike datasentrene som er sammenkoblet via et sikret nett. Sikret nett vil si at kommunikasjonen mellom servere er kryptert. Skyløsningen kan bidra til å gjøre data mer tilgjengelig. Den største verdien til skyløsningen er skalerbarheten dersom behovet for databehandlingen varierer og at NVE betaler for den kapasiteten de benytter seg av. Organisasjoner som stiller spesielle krav til informasjonslagring har mulighet til å lagre data på norsk jord. Både den fysiske og den virtuelle sikkerheten har en svært høy grad av sikring. Den fysiske sikringen krever at ansatte i tillegg til nøkkelkort må identifisere seg ved hjelp av biometriske nøkler. Et eksempel på biometrisk nøkkel kan være fingeravtrykk, iris, ansikt eller håndavtrykk. Den virtuelle sikkerheten blir ivaretatt ved at fageksperter overvåker dataen kontinuerlig. Microsoft Azure benytter kunstig intelligens til å overvåke mer enn 6,5 milliarder hendelser hver eneste dag [10]. Et kunstig intelligent system kan utføre handlinger både fysisk og/eller digitalt, den kan baserer seg på tolkninger og bearbeider data for å nå et spesifikt mål [11].

Digitaliseringsprosessen som NVE nå ønsker å iverksette skal gå ut på å forbedre dagens teknologi ved å øke tilgjengeligheten til data, effektivisere sine arbeidsoppgaver, gi bedre beslutningsgrunnlag og samvirke med andre interessenter i høyere grad. NVE er avhengig av digitale verdikjeder som strekker seg over flere sektorer. Den største sårbarheten er som Nasjonal Sikkerhetsmyndighet (NSM) sier kompleksiteten i det norske digitale samfunnet, og

ved implementering av komplekse digitale løsninger kommer det flere sårbarheter. Digitaliseringen resulterer i at koblingene blir mer sammensatte, hvor det kan være utfordrende å skille avhengighetene til enhetene. Digitale målere som NVE ønsker å implementere skal erstatte målere som tidligere ikke har vært koblet til nett. Dette vil øke avhengigheten til at systemer og teknologien fungere til enhver tid. Bærbare enheter som digitale målere er, ifølge NSM, noe som angripere spesielt søker og utnytter som inngangsportal til NVEs hoveddatabase [12].

2.1 Overvåkingsteknologi for ustabile fjellparti

NVE utfører sanntidsovervåking ved å benytte seg av følgende måleinstrumenter: Global Navigation Satellite System (GNSS), bakkebasert radarmåling (BG-InSAR), satellittbasert radarmåling (SB-InSAR), laser, totalstasjon, ekstensometer, tiltmeter, værstasjon, borehullinstrument, seismikk, strekkstag og webkamera. En mer detaljert beskrivelse av måleinstrumentene finnes vedlagt. Hvor hvert av fjellpartiene skal være utstyrt med tre eller flere uavhengige målesystem for å kunne skape redundans i overvåkningen. Overføring av måledata skjer via fiberkabler, ADSL/DSL, mobildata, satellitt og trådløs kommunikasjon[3]. Kommunikasjonen skjer via rutere og svitsjer som står ute i bunkere. Fra forskriften om tekniske krav til byggverk (TEK 17) foreligger det et krav som tilsier at sikring av skredutsatte områder krever en døgnkontinuerlig overvåkning [13].

2.1.1 Sårbarheter knyttet til overvåkingsteknologien

For å overholde kravet om kontinuerlig døgnovervåkning er det avgjørende at man er bevisst på potensielle sårbarheter som kan påvirke kapabiliteten til overvåkningen. Det er kritisk dersom svikt i måleinfrastrukturen skulle oppstå, det er derfor blitt lagt vekt på uavhengigheten mellom de ulike måleinstrumentene som en redundant løsning dersom et av instrumentene skulle svikte. Sårbarheten kan skje som følge av tilsiktede og utilsiktede hendelser.

Forstyrrelser av signaloverføring

Måleinstrumentene som blir berørt av forstyrrelser ved signaloverføring er de satellittbaserte målingene. Det vil være GB-InSAR, SB-InSAR og GNSS som er sårbare for forstyrrelser fra andre signaloverføringer. Relevant for dette studiet er hovedsakelig to metoder for å forstyrre signaloverføringen på: jamming og spoofing. I risikoanalysen vil dette omtales som

[3] SVF (2020) *PowerPoint presentasjon «Senter for fjellskredovervåking Stranda, Seksjon for fjellskred»* NVE

interferens. Når man jammer signalet betyr det at en sender ut støysignaler der hvor mottaker er plassert med den aktuelle frekvensen slik at det forstyrrer eller hindrer signalet i å komme frem til mottaket. Spoofing går ut på å sende ut falske signaler som vil manipulere tidsinformasjonen og aktuell posisjon til reflektoren [14]. Jamming kan skje som følge av en utilsiktet hendelse eller ved bruk av jammeutstyr med den intensjonen å forstyrre signalet. Spoofing er en tilsiktet hendelse med en målrettet agenda om å gi misvisende informasjon. Konsekvensen til forstyrrelse av signaloverføring kan by på store samfunnsmessige konsekvenser dersom feil ikke detekteres og nødvendig tilstandsinformasjon ikke fremkommer [15].

Klimatiske utfordringer

Det er ingen tvil om at Norge er et værhardt land, hvor en kan oppleve å ha flere årstider på en og samme dag. Sårbarheter knyttet til klimatiske utfordringer skjer som følge av vær som blokkerer mottaket av signal. Dette kan føre til at måleinstrumenter ikke får utført sin tiltenkte funksjon. Værfenomenet sludd byr på store utfordringer for måleinstrumentene laser, totalstasjon, InSAR (både GB og SB) hvor en er avhengig av å lese en avstand mellom to objekter. Tett tåke vil også skape utfordringer for webkamera som krever sikt for å kunne utføre sin funksjon [16]. Ekstremvær kan også by på utfordringer i form av fremkomst til måleinstrumentene for personell når det er oppdaget feil eller skal gjennomføre rutinemessig sjekk.

Vedlikehold av måleinstrumenter

Manglende vedlikehold av måleinstrumentene kan føre til at den med tid ikke vil fungere slik som tiltenkt. En av grunnen til at dette oppstår er fordi det er for farlig å opphold seg i områder der hvor denne innretningen er plassert, det kan også oppstå som følge av at det ligger i et ulendt område hvor fremkomst ikke er mulig. Ekstensometer og strekkstag er typiske innretninger som kan befinne seg på ulendte områder som ikke lett lar seg vedlikeholdes knyttet til utfordringer med fremkomst og området [17].

Fysiske ødeleggelser

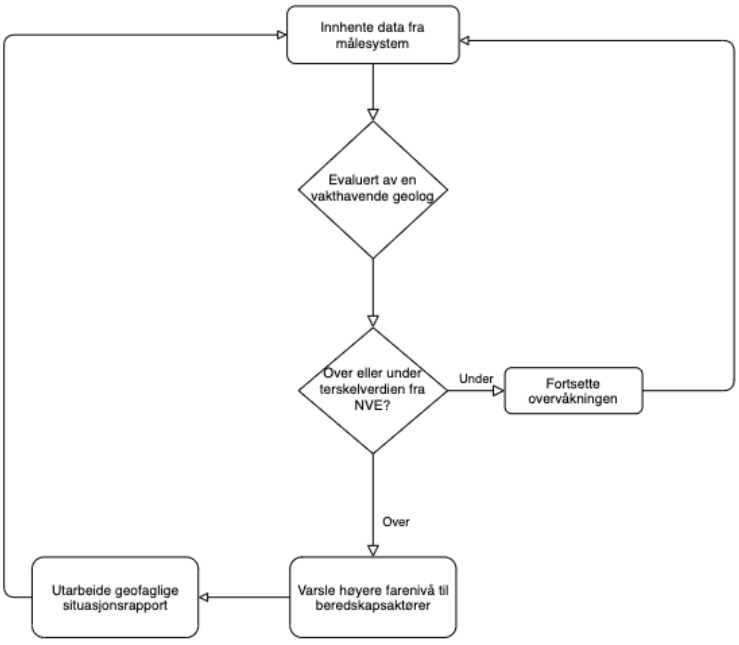
Det knyttes også en sårbarhet til instrumentenes robusthet. Fysiske ødeleggelser skjer som følge av en tilsiktet eller utilsiktet hendelse. Draw-wire og crackmetere er skjøre instrumenter som ikke tåler store fysiske påkjenninger. Strømkabler ut til måleinstrumentene er også skjøre

for fysisk påkjenning, noe som kan føre til at strømtilførselen til måleinstrumenter kan bli brutt som følge av at kablene blir ødelagte [18].

2.2 SKRED OG SKREDVARSLING

Et skred oppstår ved hurtig forflytting av tørre eller våte masser nedover en skråning. En kan dele skred inn i tre kategorier: snøskred, fjellskred og løsmasseskred. I dette studiet er fokuset kun på fjellskred, som blir betegnet som det største skredet av de tre kategoriene. Dersom 100 000 kubikkmeter eller mer av et fjell raser ut blir det kategorisert som et fjellskred. Årsaken til fjellskred er komplekse og sammensatt av flere faktorer, blant annet dyptgående sprekkdannelser i berggrunnen. Sprekkene kan også utvikles over tid som følge av svakhetsstrukturer i berggrunnen som kommer av kjemisk og fysisk forvitring [19]. Forvitring er nedbryting av bergarter, mineraler, jordsmonn og andre materialer ved direkte kontakt med luft, vann, temperatursvingninger og biologiske organismer [20].

Ansvarsoppgavene NVE har innen skredforebygging er å bistå kommuner og samfunnet med sin kompetanse samt ressurser til kartlegging, arealplanlegging, sikring, overvåking, varsling og beredskap. For å kunne forebygge skredulykker på en forsvarlig måte har NVE ansvaret for å drifte landsdekkende skredvarsling. Dette skal bidra til å iverksette tiltak som kan forebygge uønskede hendelser på liv, helse og andre verdier. Varslingssystemet er en operativ nasjonal overvåkningstjeneste som baserer seg på bruk av hydrometeorologiske sanntidsdata fra målestasjoner i mulige utsatte området. Overvåkningen av skredutsatte områder er et samarbeid mellom NVE, Statens vegvesen, MET, Bane NOR, NGU og SVF [9].



Figur 2.2 Flytskjema for skredvarsling

Terskelverdien er en sammensatt verdi av innsamlet kunnskap knyttet til det aktuelle skredområdet. Ved et fjellskred vil hastigheten kunne avgjøre om det overgår terskelverdien. En sentral del av det å sette terskelverdi er å utarbeide scenarioer. Der man kan se på de historiske dataene, som i kombinasjon med værmeldinger, skal kunne si noe om hvordan situasjonen vil se ut i nær fremtid. NVE innhenter store mengder data som skal ses i sammenheng med de historiske dataene [21].

Fjellskredovervåkning/-varsling

I Norge er det kartlagt sju ustabile fjell som overvåkes døgnkontinuerlig. Utsatte fjellpartier blir overvåket med hjelp av tre eller flere uavhengige målesystemer. Sanntidsdataen blir kontinuerlig evaluert av kompetente fagpersoner i form av geologer, mens målesystemene og den tilhørende infrastrukturen blir kontrollert av teknikere. Sanntidsdataen fra tre eller flere målesystem blir sendt til to overvåkingssentre som er kontinuerlig bemannet. De er lokalisert i Stranda i Storfjord og Kåfjord i Troms. Dersom målinger viser antydninger til endring av farenivået vil det påvirke beredskapsnivået. Ved endringer har NVE i oppgave å varsle andre beredskapsaktører. Det kan være kommuner, politi, fylkesmannen, der endring i farenivå, også byr på endring av beredskapsnivå. De sju ustabile fjellpartiene per 2020 er Joasetbergi i Sogn og Fjordane, Åknes i Møre og Romsdal, Hegguraksla i Møre og Romsdal, Mannen i Møre og Romsdal, Jettan i Troms, Indre Nordnes i Troms og Gámanjunni 3 i Troms. Dette er såkalte høyrisikoobjekter i Norge som har en døgnkontinuerlig overvåkning [9]. For objekter med lavere risikonivåer foregår det en periodisk overvåkning, antall fjellparti med periodisk overvåkning er per dagsdato 11 (2020). Den periodiske overvåkningen blir utført av SVF, og er tilpasset for hvert enkelt risikoobjekt [21].

2.3 DEN DIGITALE VERDIKJEDEN

En sentral del av studiet er å kartlegge den digitale verdikjeden. En digital verdikjede kan defineres som «*en struktur av leveranser mellom virksomheter, hvor hver leveranse enten er en digital tjeneste, software eller hardware*» [22, p. 10]. Digitaliseringen byr på mer komplekse verdikjeder, hvor en kan oppleve å miste oversikten over avhengigheten til leverandører og digitale tjenester. Avhengigheten kan også en rotårsak til sårbarhetene som ligger latent betingelser i verdikjeden, spesielt når den digitale verdikjeden også er transnasjonal. Transnasjonale verdikjeder strekker seg over landegrenser, og kjennetegnes ved at ulike deler av den kan være underlagt andre staters jurisdiksjon. Dette betyr at norske

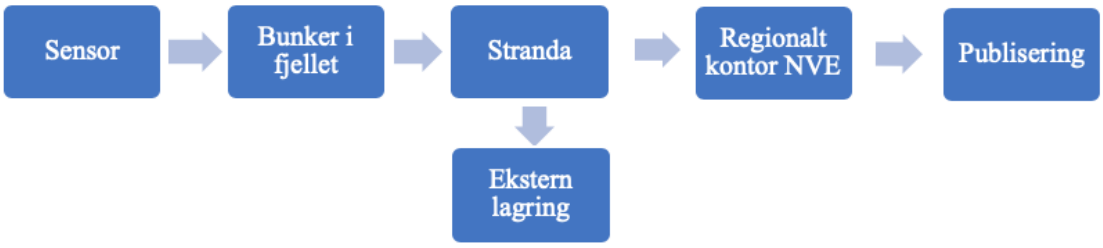
myndigheter i begrenset grad har mulighet til å påvirke hvordan sikringsarbeidet blir utført [22]. En digital verdikjede kjennetegnes ved at [22]:

- Feil oppstår på en uforventet måte, hvor feilen kan spre seg momentant
- En tjeneste som er en del av den digitale verdikjeden er tverrsektoriell, hvor tjenesten også er underlagt ulike lovverk og tilsynsregimer
- Øverste ledd av den digitale tjenesten har store utfordringer med å kartlegge sårbarheter for hele verdikjeden til tjenesten

Varslingstjenesten for skred er en digital tjeneste som befinner seg i enden av en digital verdikjede, som består av flere leverandører og underleverandører. Tjenesten er nettportalen varsom.no som driftes av NVE i samarbeid med Statens vegvesen og meteorologisk institutt [23]. En oversikt over varslingstjenestens verdikjede er helt nødvendig for å kunne se hvordan sårbarhetene kan oppstå. I tillegg for å kartlegge hvilke avhengigheter tjenesten har for å kunne skape redundans og unngå eskalering. Den digitale verdikjeden til skredvarsling består av; interne oppgaver, transnasjonale leverandører og eksterne leverandører. Hensikten oppdelingen ligger i behovet for en oversiktlig risikoanalyse opp mot de ulike verdikjedene. Risikoanalysen ligger vedlagt.

2.3.1 INTERN VERDIKJEDE FOR SKREDVARSLING

Den interne verdikjeden kan forstås som et eget system NVE har for å overvåke skredutsatte områder, hvor informasjonen blir distribuert lokalt og innenfor NVEs rammer.



Figur 2.3.1 Intern digital måleverdikjede for fjellskredvarsling

Det første leddet i verdikjeden består av datainnsamling fra ulike sensorer som skal detektere anormale målinger i skredutsatte områder. Sensorene er avhengig av strømtilførsel og får det fra tre aggregater plassert inne i fjellet. Måledata blir deretter distribuert trådløst og via kabel til bunkere som er utstyrt med feltpc og loggere som blir oppbevart i zargeskasser og skap. Neste steg i verdikjeden er distribusjon av måledata fra bunkerne til Strandas

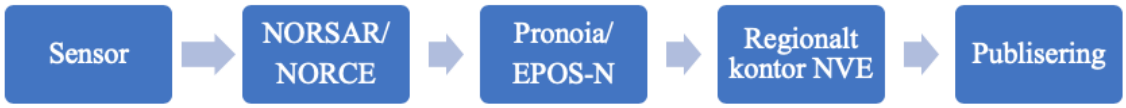
overvåkingssenter speiler backup av måledata for ekstern lagring. Personell fra overvåkingssenteret sender informasjon til geologer for videre analyse på plattformen Cautus Web. Cautus Web er et modulbasert databehandlingssystem som skal bistå til å benytte riktig informasjon i sanntid fra ulike sensorer og instrumenter, og driftes av eksterne leverandører [24]. Geologer utarbeider daglig interne tekniske og geologiske rapporter, og ved slutten av hver vakt på mandager blir informasjonen sammenstilt med andre måledata fra MET, Statens vegvesen og Bane NOR som deretter blir publisert på varslingsportalen varsom.no [23].

	Innhenting av data		**Dataprosessering**			**Resultat av analysert data**
Ledd	Instrument	Bunker i fjellet	Stranda	Ekstern lagring	Regionalt kontor NVE	Publisering
Støtteprosesser	• GNSS • Laser • Totalstasjon • Crack og ekstensometer • Tiltmeter • Værstasjon	• Loggere • Feltpc	• Bearbeiding av måledata	• Back-up måledata	• Cautus Web • Rapport • Azure	• Sammen-stilte måleverdier presentert på varsom.no

Tabell 2.3.1 Oversikt intern digital måleverdikjede for fjellskredvarsling

2.3.2 NORSK LEVERANDØR VERDIKJEDE FOR SKREDVARSLING

Norsk leverandør verdikjede kan forstås som en verdikjede hvor en ekstern norsk aktør er involvert i ett eller flere ledd av verdikjeden for skredvarsel.



Figur 2.3.2 Norsk leverandør digital måleverdikjede for fjellskredvarsling

Den digitale verdikjeden starter på samme måte som den interne verdikjeden ved at sensorer innhenter måledata fra utsatte fjellparti. Forskjellen mellom den interne verdikjeden og norsk leverandør verdikjeden er type instrumentering det er brukt for å innhente måledata. Instrumentene geofoner og seismometer sender informasjon til eksterne leverandør NORSAR for videre analyse av rystelser og trykkbølger. NORSAR har kjernekompetanse innen seismologi og samarbeider med NVE for å overvåke ustabile fjellparti [25]. Instrumentet SB-InSAR sender informasjon til NORCE for prosessering og presentering av data. NORCE er et

statlig forskningsinstitutt som utvikler prototyper av syntetisk aperture radar (SAR) overvåkningssystemer til å detektere blant annet skred [26]. NORSAR og NORCE bearbeider data og presenterer data på hver sin portal. NORSAR presentere sine data på nettportalen EPOS-N, mens NORCE publiserer sine data på nettportalen Pronoia. Publisert data blir analysert av geologer og teknisk personell fra NVE og SVF. Personell fra regionale kontorer i seksjon for fjellskred anvender måledata publisert på Pronoia og EPOS-N fra tekniske og geologiske rapporter og sammenstiller med måledata fra MET, Statens vegvesen og Bane NOR og som deretter blir publisert på nettportalen varsom.no.

	Innhenting av data	**Dataprosessering og presentering av måledata**			**Resultat av analysert data**
Ledd	Instrument	NORSAR/ NORCE	Pronoia/ EPOS-N	Regionalt kontor NVE	Publisering
Støtteprosesse	• Geofoner • Seismometer • SB-InSAR	• Prosessering og presentering av data	• Radardata blir overført fra NORCE til Pronoia • Seismikkdata blir overført til EPOS-N	• Rapport • Azure	• Sammen-stilte måleverdier presentert på varsom.no

Tabell 2.3.2 Oversikt norske leverandører digitale måleverdikjeden for fjellskredvarsling

2.3.3 TRANSNASJONAL VERDIKJEDE FOR SKREDVARSLING

Transnasjonal verdikjede strekker seg ut av landet gjennom internasjonale eksterne aktører, som byr på andre utfordringer spesielt knyttet til andre lands jurisdiksjon.

Figur 2.3.3 Transnasjonal digital måleverdikjede for fjellskredvarsling

Data fra instrumentene GB-InSAR, SB-InSAR og borehullsinstrumentering overføres til de italienske selskapene Ellegi LiSALab og CSG Engineering. Ellegi LiSALab leverer tjenester som relateres til radarovervåkningen GB-InSAR og SB-InSAR [27] for risikoutsatte fjellparti. CGS Engineering produserer borehullsinstrumenter med differensialmålinger som hjelper NVE i å overvåke de risikoutsatte fjellpartiene [28]. Bearbeidet data blir presentert på leverandørenes portal. Måledataen blir oversendt til NVEs server i Oslo [1]. Deretter henter regionalt kontor ut nødvendig data som blir grunnlaget for en rapport. Geologer og teknisk

personell fra NVE anvender informasjonen og sammenstiller måledata fra MET, Statens vegvesen og Bane NOR for så å publisere informasjonen på varslingsportalen varsom.no.

	Innhenting av data	**Dataprosessering og presentering av måledata**			**Resultat av analysert data**
Ledd	Instrument	Italia	NVE Oslo	Regionalt kontor NVE	Publisering
Støtteprosesse	• GB-InSAR • Borehull-instrument	• Prosessering og presentering av data	• Radardata overført til server i Oslo og presentert på portal	• Rapport • Azure	• Sammen-stilte måleverdier presentert på varsom.no

Tabell 2.3.3 Transnasjonale leverandører digitale måleverdikjeden for fjellskredvarsling

2.4 SÅRBARHETER OG TRUSLER

I den årlige nasjonale trusselvurderingen[4] fra PST kommer det frem at det er en stadig økning i antall enheter som kobles til internett. Dette medfører et økt antall bakdører som potensielle trusselaktører kan finne og hacke seg inn i. For NVE som ønsker å koble opp digitale målere i måleinfrastrukturen vil det potensielt føre til mer sårbarheter. Brukere av målesystemet stoler på at den oppgitte informasjonen er gyldig. Ta utgangspunkt i høyrisikoobjektet Mannen, det ustabile fjellpartiet i Rauma, som er under kontinuerlig overvåkning. Dersom trusselaktører ønsker å sabotere måleinfrastrukturen som overvåker Mannen kan det potensielt føre til at sikringstiltak ikke blir iverksatt tidlig nok. Sikringstiltak som evakuering kan skje for sent, og i ytterste konsekvensene kan det føre til at 1650 av befolkningen bosatt i Rauma blir utsatt for en flodbølge. Denne situasjonen er høyst aktuell da både statlige og ikke-statlige aktører er ute etter Norges naturressurser på bakgrunn av at Norge er leverandør av kraftforsyning til andre land [8].

Varslingsportalen varsom.no er en tjeneste som befolkningen kan benytte seg av for å vurdere hvorvidt det er trygt å oppholde seg i skredutsatte område [23]. Blir denne tjenesten kompromittert kan det føre til at viktig informasjon om skredutsatte områder ikke blir formidlet, som da igjen kan påvirke befolkningens vurdering av trygg ferdsels i skredutsatte området. Feilinformasjon fra målesystemene kan få alvorlige konsekvenser. Derfor må sårbarhetene til målesystemene være kartlagt og analysert for å kunne iverksette riktig sikringstiltak. Men når målesystemer er sammensatt av mange ulike enheter fra flere kilder vil

[4] PST (2020) *Nasjonal trusselvurdering 2020*

arbeidet med å identifisere hvor sikkerhetsbruddet skjedde være problematisk. Kompleksiteten til et målesystem med mange tilhørende påkoblede enheter gir utfordringer i sikkerhetsarbeidet. For å få systemet raskest mulig tilbake i normalsituasjon må det kunne kartlegges hvor sikkerhetsbruddet skjedde og hvilken enhet som er kompromittert [29].

Kontroll over energiforsyningen vil være en maktfaktor som er attraktiv for andre statlige aktører. Ifølge PST sin trusselvurdering[5] er utenlandske etterretningstjenester høyst aktuell til å ville infiltrere ansatte i norske virksomheter. Ved å samle inn kontaktinformasjon kan de for eksempel bruke metoder som avlytting og nettverksinfiltrasjon. De er også interessert i å stjele sensitiv informasjon fra norske virksomheter. Konsekvensen av denne spionasjen mot norske virksomheter, og da spesielt for NVE, er tap av konfidensialitet. Ifølge trusselvurderingene er målrettet angrep mot NVEs informasjonsforvaltning interessant for mange aktører. *«Norge har naturressurser av stor betydning for energiforsyningen til andre stater. Dette er en maktfaktor, derfor ønsker andre stater innsikt i norsk energisektor»* [29, p. 8]. Angrepene kan føre til tap av samfunnets kapabilitet med mer alvorlige konsekvenser som tap av vannforsyning til befolkningen. Dagens angrep kan utføres med såpass høy anonymitet og skje helt tilfeldig slik at det er vanskelig å kartlegge hvem trusselaktøren er og forutsi når angrepet kommer [29].

En annen aktuell trusselaktør for NVE er «innsideren» som er en person med kjennskap til systemet og har adgang til verdifull informasjon. Trusselvurderingen fra PST definerer en innsider som «*en person som utnytter, eller har intensjon om å utnytte, sin legitime tilgang til en virksomhets verdier til uautoriserte formål»* [29, p. 10]. Formålet til innsideren kan enten være å selge sensitiv informasjon som svekker NVEs omdømme, eller sabotere kritiske infrastrukturer ved å manipulere informasjon som for eksempel blir publisert på varsom.no. Innsideren kan finnes i hele verdikjeden. Utenlandske etterretningstjenester kan eksempelvis forsøke å rekruttere tidligere ansatte, da sannsynligheten for å lykkes med å tilegne seg sensitiv informasjon fra de er større for de enn hos nåværende ansatte [29].

3 KAPITTEL: TEORI

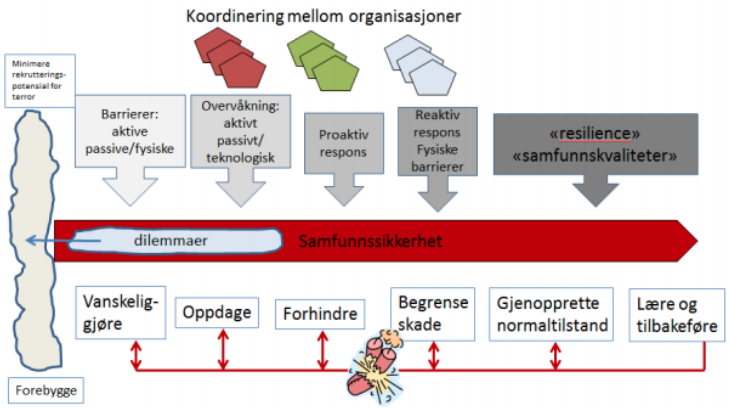
Dette kapittelet presenterer det teoretiske rammeverket som studien er bygget opp rundt. Utvelgelsen av teorien tar utgangpunkt i å øke leserens forståelse for hva som kommer i

[5] PST (2020) *Nasjonal trusselvurdering*

analysen og skal gi leseren nok kunnskap til å forstå sammenhengen mellom problemstilling, diskusjonen og den avsluttende konklusjon.

3.1 SAMFUNNSSIKKERHET

Samfunnssikkerhet handler om evnen til å opprettholde kritiske samfunnsfunksjoner, og kapabiliteter som ivaretar menneskers liv og helse under ulike ytre påkjenninger. Slike ytre påkjenninger kan være tilsiktede eller utilsiktede. Tilsiktede hendelser kan være terror, hacking, fysisk ødeleggelser eller andre ondsinnede handlinger. Utilsiktede hendelser kan være naturskapte, menneskelige feilhandlinger eller teknisk svikt. En modell utviklet for å vurdere samfunnssikkerhet bygger på den kjente teorien fra Rasmussens forsvar-i-dybden og Tuners modell over ulike hendelser og dets følgende hendelsesforløp. I tillegg til Reasons sveitserostmodell for barrierer med latente betingelser. Schifloe (2011) har med utgangspunkt i teorien fra Rasmussen, Reasons, Turner og Resilience Engingeering utviklet en modell for å vurdere samfunnssikkerhet [30].



Figur 3.1.1 Holistisk tilnærming til samfunnssikkerhet [30]

Modellen viser en holistisk tilnærming til å vurdere samfunnssikkerhet. Hovedmålet til den holistiske modellen er å få et grunnlag for å vurdere både tilsiktede og utilsiktede hendelser på et overordnet nivå. Hovedaktivitetene fra modellen går ut på å komme med forebyggende tiltak, vanskeliggjøre for å realisere ondsinnede handlinger, oppdage ved å detektere unormal aktivitet, forhindre ved å være proaktiv i respons på unormal aktivitet, skadebegrensende tiltak og normalisere for å gjenopprette normaltilstand [30].

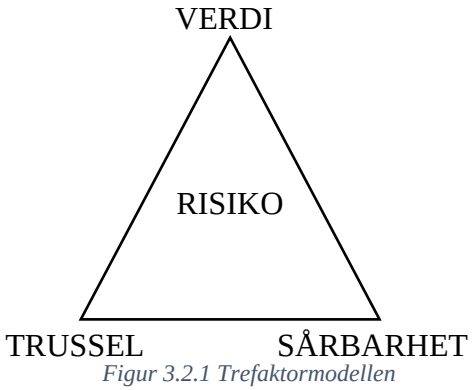
3.2 RISIKO

Risiko er et begrep som kan forstås som en kombinasjon av faktorene verdi, trussel og sårbarhet [31]. Risiko er beheftet med en viss form for usikkerhet som man ikke kan komme unna, enten det er i form av en trusselaktør eller motivasjonen for angrepet. Det eksisterer

mange ulike tilnærminger og definisjoner av begrepet risiko. En tilnærming til begrepet som er relevant å bruke for dette studiet er at «*risiko ses på som en kombinasjon av mulige konsekvenser med en tilhørende sannsynlighet*» [1, p. 35]. Man kan benytte ulike risikoindekser for å beregne en risiko. I dette studiet blir konsekvensen multiplisert sammen med sannsynlighet for å fremstille den sammenlagte risikoen. Det er også viktig å vite at risikoen vil være avhengig av foreliggende informasjon og kunnskap om fenomenet. Ved stor usikkerhet knyttet til risikoen vil det være vanskelig å gi gode vurderinger av fremtidige konsekvenser. Derfor kan en løsning være å legge vekt på en samfunnsmessig verdivurdering, som i denne studien er ekspertkunnskap [1].

3.2.1 TREFAKTORMODELLEN

Risiko ble tidligere beskrevet som en kombinasjon av verdi, trussel og sårbarhet, denne kombinasjonen er også kjent under navnet trefaktormodellen. Modellen er et nyttig overordnet verktøy for å vurdere risiko. Faktorene kan brukes til å vise til en relasjon for å utarbeide konsekvensutredning ved å vurdere risikoen opp mot verdien, trusselen og sårbarheten til en aktuelle farekilden. Et eksempel kan være en verdi som er sårbar, men som ikke har en reell trussel. Det kan også være en kritisk verdi som er har en alvorlig trussel rettet mot seg, men som ikke har sårbarhet [32].



Figur 3.2.1 Trefaktormodellen

VERDI

Når man snakker om verdier i et cybersikkerhetsperspektiv vil dette være verdier som informasjon og arbeidsprosesser, dette er primærverdiene til cybersikkerhet [32]. Et eksempel på verdi for NVE kan være skjermingsverdig informasjon som kraftsensitive opplysninger. Skjermingsverdig informasjon er definert som «*sikkerhetsgradert informasjon hvor konfidensialitet må beskyttes av hensyn til nasjonale sikkerhetsinteresser* [33, p. 3]«. Sekundærverdiene som blir vurdert er hardware, software, nettverk, personell, arbeidsområdet

og organisasjonsstruktur [32]. Det er i all hovedsak verdiene som er attraktive for trusselaktørene, og verdiene utgjør et viktig grunnlag for dannelse av gode sikringstiltak.

TRUSSEL

Trussel beskriver en potensiell hendelse som kan føre til enten en utilsiktet eller tilsiktet hendelse hvor verdiene til organisasjonen blir berørt. For begrepet trussel er det i cybersikkerhetsperspektivet det vanlig å skille mellom tre ulike typer: utilsiktede hendelse, tilsiktede angrep og målrettet tilsiktede angrep [6]. Utilsiktede hendelser skjer som følge av en «naturlig» hendelse som en menneskelig feil eller teknisk svikt. Denne feilen kan oppstå som følge av ekstremvær, eller glipp i prosedyren som fører til en feil i systemet. For å redusere sannsynligheten til denne type risiko vil det å ha god sikkerhetskultur være viktig for å forebygge menneskelige feilhandlinger. I tillegg til å ha et system med innebygd redundans dersom for eksempel ekstremvær skaper en teknisk svikt. Tilsiktede angrep er et mer generelt angrep på IKT-systemer, hvor den som utfører angrepet ikke retter seg direkte mot en spesifikk bransje. Malware er den vanligste formen for ondsinnet programvare som enten kan forplante seg dersom ansatte følger instrukser gitt på mail, eller logger seg inn på en tilsynelatende fortrolig side, men som er kompromittert. For å redusere risikoen ved tilsiktede angrip er det også viktig med en god sikkerhetskultur, som går ut på å informere og opplyse ansatte om å se etter mistenksomme nettsider, e-poster og programmer. Målrettede tilsiktede angrep retter seg inn mot en spesifikk bransje og en spesifikk funksjon i et IKT-system [6].

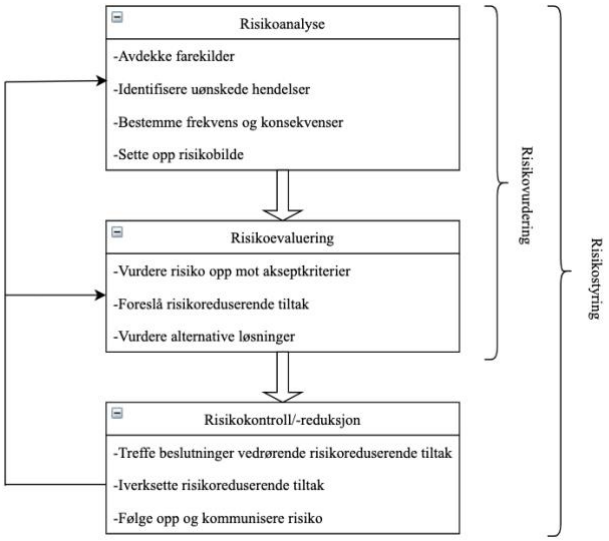
SÅRBARHET

Sårbarhet i cybersikkerhet vil man kunne forstå som en svakhet i systemet hvor en angriper har mulighet til å utnytte sårbarheten for å få tilgang til verdier. En definisjon av begrepet sårbarhet som er relevant for studiet er «*et uttrykk for de problemer et system får med å fungere når det utsettes for en uønsket hendelse, samt de problemer systemet får med å gjenoppta sin virksomhet etter at hendelsen har inntruffet*» [34, p. 31]. Denne sårbarheten kan eksistere som en latent betingelse eller blir tilført som følge av ny implementert teknologi, uten tilstrekkelig risikovurderinger.

3.3 RISIKOSTYRING

Risikostyring er en metode for å redusere risikoen ved å benytte sikringstiltak som enten er sannsynlighetsreduserende eller konsekvensreduserende. Sikringstiltakene er enten tekniske, operasjonelle eller organisatoriske tiltak som reduserer sannsynligheten eller konsekvensen av den uønskede hendelsen. Risikostyringsprosessen går ut på å velge best egnet sikringstiltak til

den uønskede hendelsen som blir kartlagt i startfasen av prosessen. Risikostyringsprosessen kan se slik ut [35]:

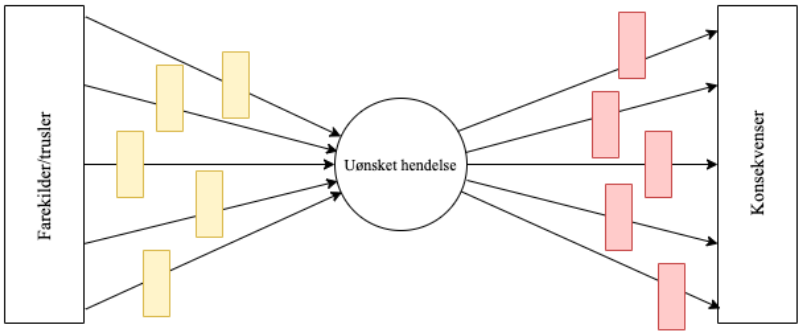


Figur 3.3.1 Forenklet bilde av de ulike elementene i risikostyringsprosessen [41]

Figuren 3.3.1 viser hvilke aktiviteter som inngår i risikostyringsprosessen der risikoanalyse, risikoevaluering og risikokontroll/-reduksjon inngår som hovedelementene. En risikoanalyse er et metodisk verktøy for å avdekke, identifisere og fremstille farekilder. Det eksisterer mange former for risikoanalyser, det gjør utvelgelsen av den mest egnede veldig viktig. Derfor må planleggingsfasen ta hensyn til hvilket system som skal vurderes slik at resultatet blir best mulig, og at risikoanalysen gir den opplysningen som etterspørres.

3.3.1 ISO 31000- RISIKOSTYRING

En risikometode som ofte benyttes for å kartlegge en helhetlig risikovurdering av et system er ISO 31000 sitt rammeverk for risikostyring, og kan ses på som en tradisjonell risikometode. Hensikten med å benytte ISO 31000 standarden er å skape et mer resilient system. Begrepet resiliens kommer til å bli definert under kapittel 3.5.1. En modell som illustrerer risikostyringen er den kjent bow-tie-modellen som bygger på Rasmussens teori om et forsvar-i-dybden, og tar for seg sannsynlighetsreduserende og konsekvensreduserende tiltak. Bow-tie-modellen skal identifisere flere initierende hendelser som kan føre til den uønskede hendelsen, og den skal også beskrive konsekvensene dersom den uønskede hendelsen inntreffer. I forbindelse med bow-tie blir begrepet barrierer brukt for å beskrive tiltak for å enten redusere sannsynligheten for at den uønskede hendelsen skjer, eller konsekvensen av den. Bow-tie modellen tar utgangpunkt i Turners (1978) teori om menneskeskapte katastrofer. Ifølge teorien kan man ved å betegne ulykkene også si noe om hvordan hendelsesforløpet vil forvitre seg, og dermed ha større sannsynlighet for å hindre eskalering av hendelsen [36].



Figur 3.3.2 Bow-tie-modellen

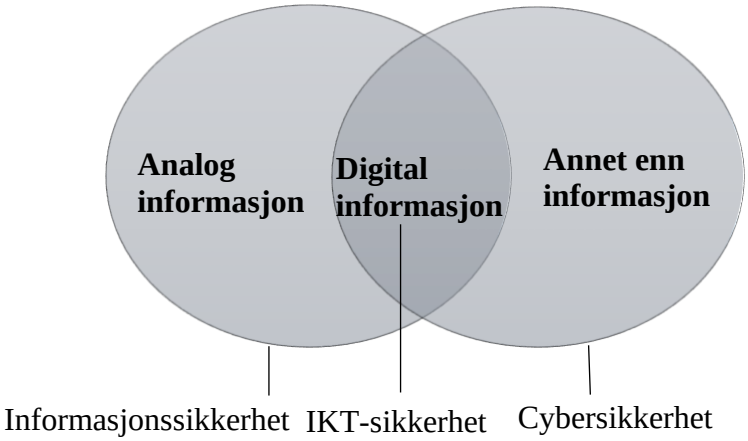
Figur 3.3.2 illustrer bow-tie-modellen hvor de initierende hendelsene blir kartlagt til venstre under farekilder/trusler. De gule boksene representerer proaktive barrierer. De røde boksene representerer reaktive barrierer, samt konsekvensen av den uønskede hendelsen. Bow-tie-modellen viser en årsakskjede til hendelsen, hvor det er en gitt situasjon som utspiller seg på en tiltenkt måte. Slike analysemetoder fungere godt der kunnskapen om konsekvensen er kjent og historiske data kan stadfeste en reell sannsynlighet. Analysemetoden gir en god indikasjon på sårbarheter i et system, men det helhetlige bilde hvor flere komponenter samvirker på en ny måte blir noe vanskelig å kartlegge i denne lineære risikoanalysemetoden [35].

Fra bow-tie fremstillingen kan man gå videre til grovanalysen. Grovanalysen er en allsidig analyse som ved enkle grep kan tilpasses til cybersikkerhet, analysen er enkel å tolke og lar seg gjennomføre dersom mengden relevant data er å oppdrive. Kritikk til analysen er at det kun gir et stillestående bilde av en situasjon som i realiteten er et dynamisk system, og derfor vil analysen kun svare til tilstanden ved gjennomførelse av analysen. Med tanke på den raske utviklingen innenfor IKT-systemet vil det ikke ta lang tid før analysen ikke lengre svarer på farekildene i det fremtidsrettede IKT-systemet. Grovanalysen gir også anbefalinger for risikoreduserende tiltak som kan motvirke eksisterende tiltak, og dermed føre til en uønsket hendelse [35].

3.4 CYBERSIKKERHET

Cybersikkerhet kan forstås som «*et potensiale for at en gitt trussel vil utnytte sårbarheter for å få urettmessig tilgang til en verdi eller gruppe av verdier og dermed forårsake skade på organisasjonen*» [32, p. 1]. Cybersikkerhet er et begrep som rommer flere dimensjoner enn informasjonssikkerhet og IKT-sikkerhet. Begrepet cybersikkerhet omfatter med andre ord

ikke bare beskyttelse av informasjon, men også alt som er sårbart relatert til IKT. Det vil si at både tekniske og menneskelige hendelser kan potensielt være sårbare i IKT-sikkerheten. For å vurdere cybersikkerheten kan en anvende CIA-triaden som et sikkerhetsmål på hvordan verdiene kan bli kompromittert. CIA-triaden står for konfidensialitet, integritet og tilgjengelighet. Konfidensialitet i et cybersikkerhetsperspektiv betyr at informasjon skal holdes hemmelig, der kun autoriserte brukere får tilgang til den klassifiserte informasjonen. Integritet skal sikre at informasjonen som blir anvendt er riktig, at den er oppdatert og at leseren kan stole på kilden til informasjonen. Tilgjengelighet viser til at informasjonen skal være tilgjengelig for de rette brukerne av systemet og at dette systemet fungerer til enhver tid [12].



Figur 3.4.1 Konseptualisering av begrepene cybersikkerhet, IKT-sikkerhet og informasjonssikkerhet [62]

Det er elementer med cybersikkerhet som gjør det utfordrende å gjennomføre en tradisjonell risikoanalyse. Cybersikkerhet blir i større grad styrt av tilsiktede hendelser som gjør hendelsesforløpet noe uforutsigbart ved at konsekvens blir subjektivt og kan variere fra gang til gang. Sannsynligheten kan også være problematisk å kartlegge for en tilsiktet hendelse innenfor cybersikkerhet. Det er utarbeidet flere sjekklister og tilnærminger for å vurdere cybersikkerhet, blant dem er forskningsprosjektet[6] «Sårbarhet i kritiske IKT-systemer». Forskningsprosjektet har utarbeidet en metode for å gjennomføre risikoanalyse av samfunnskritiske IKT-systemer. Ifølge rapporten helt nødvendig med kompetanse innen systemets funksjonalitet, tilknyttede komponenter, anvendt programvare og eksisterende sikringstiltak.

[6] Forsvarets forskningsinstitutt (2007) *Beskyttelse av samfunnet 5: Sårbarhet i kritiske IKT-systemer - sluttrapport*

3.4.1 RAMMEVERK FOR CYBERSIKKERHET

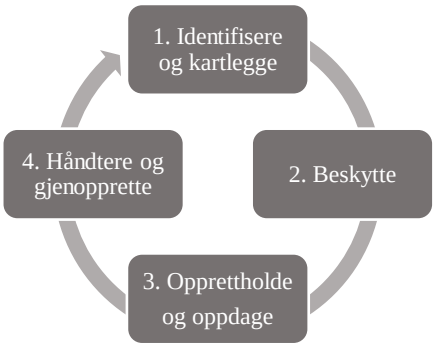
En måte å kontrollere cybersikkerheten på er å utvikle rammeverk for hvordan man skal håndtere cyberhendelser. Det er de siste årene utviklet flere rammeverk for hvordan man skal kunne opprettholde god cybersikkerhet i virksomheten. Det er på bakgrunn av problemstillingen valgt å ta utgangspunkt i det nasjonale rammeverket fra NSM, samt tre internasjonale rammeverk for cybersikkerhet. Den første utarbeidet av Nasjonal institutt for standard og teknologi (heretter NIST). Den andre det europeiske byrået for nettverks- og informasjonssikkerhet (heretter ENISA). Til slutt den internasjonale organisasjonen for standardisering (ISO) sammen med den internasjonale organisasjonen for elektroteknologisk kommisjon (IEC).

Rammeverk for informasjonssikkerhet
Et rammeverk for informasjonssikkerhet består av et sett av aktiviteter som skal gjennomføres for å forebygge og detektere sikkerhetsbrudd som kan kompromittere verdifull informasjon for organisasjonen. Aktivitetene skal gå ut på å gjennomføre internkontroll for de etablerte rutinene, avklare rollefordelingen med tydelige ansvarsforhold, og ha et system for rapportering av hele verdikjeden til organisasjonen. Dette rammeverket skal tilpasses hver organisasjon etter hva de opererer med, samt med de føringene som allerede foreligger som beredskapsforskriften, ISO standard, sikkerhetsloven, personopplysningsloven og internasjonale forordninger [37].

Tabell 3.4.1 Informasjonsboks om rammeverket for informasjonssikkerhet

NSMs grunnprinsipper i IKT-sikkerheten

NSM sine grunnprinsipper skal hjelpe organisasjoner med å ivareta IKT-sikkerhet ved å følge aktivitetene som inngår i grunnprinsippene, som er illustrert i figur 3.4.2. Enhver organisasjon bestemmer selv hvordan de ønsker å tolke aktivitetene og hvilke av de som skal implementeres. Bakgrunnen for at de er plassert i en sirkulær figur er for å illustrere hvordan denne prosessen kan forstås som en kontinuerlig prosess [38].



Figur 3.4.2 Et hjul som illustrerer NSMs grunnprinsipper

1. *Identifisere og kartlegge* [12]*:*

Hensikten til det første grunnprinsippet er å skape et godt grunnlag for effektiv implementering av gjenværende prinsipper. Første aktivitet er å identifisere organisasjonens infrastruktur, hvordan arbeidsoppgaver blir utført og prosessen fra rådata til brukerdata. Dette innebærer å opparbeide og forvalte forståelse om virksomheten herunder leveranser, tjenester, systemer og brukere. Kartlegg leveranser og verdikjeder, kartlegg enheter og programvare, kartlegg brukere og behov for tilgang.

2. *Beskytte* [12]*:*

Grunnprinsippet beskytte beskriver hvordan man skal etablere en sikker tilstand for de IKT-systemene. Aktiviteter som inngår er å sikre at IKT-systemene kommer fra troverdige leverandører, hvordan de planlegges å brukes, hvordan de blir bygd inn i eksisterende infrastruktur og ivareta korrekt konfigurering av enhetene slik at sikkerheten blir ivaretatt.

3. *Opprettholde og oppdage* [12]*:*

Den viktigste aktiviteten under dette grunnprinsippet vil være loggføring av teknologien for å oppdage eventuelle avvik som kan føre til en uønsket hendelse. Dette innebærer blant annet å opprettholde den sikre tilstanden over tid og ved endringer, og oppdage sikkerhetstruende hendelser. Sørge for god endringshåndtering, verifisere konfigurasjon, overvåke, analysere IKT-systemet og beskytte mot skadevare. Gjennomføre inntrengingstester og «red-team» øvelser, samt ivareta kapabilitet for gjenoppretting av data.

4. *Håndtere og gjenopprette* [12]*:*

Grunnprinsippet håndtere og gjenopprette vil fokusere på aktiviteter som forbereder virksomheter på eventuelle situasjoner der data kan bli kompromittert. Dette innebærer aktiviteter som håndtere sikkerhetstruende hendelser effektivt, forberede virksomheten på håndtering av hendelser, vurdere og kategorisere hendelser, kontrollere og håndtere hendelser, evaluere og ta lærdom av hendelser.

NIST – Rammeverk for å forbedre kritisk infrastrukturs cybersikkerhet

NIST sitt rammeverk er utarbeidet i USA for å forbedre cybersikkerheten for kritisk infrastruktur. Rammeverket er delt inn i tre hovedkategorier: rammeverket kjerne, rammeverkets nivåer og rammeverkets profil [39].

Rammeverkets kjerne (Core) består av en rekke cybersikkerhetsaktiviteter, ønsket måloppnåelse og referanser som er gjeldende på tvers av kritiske infrastruktursektorer. Gjeldende standarder sammen med retningslinjer skal muliggjøre det å kunne kommunisere cybersikkerhetsaktivitetene samt resultater gjennom hele organisasjonen, fra ledelsesnivå til implementeringsnivået. Cybersikkerhetsaktivitetene er fem sammenhengende aktiviteter som kontinuerlig skal gjennomføres, og de består av å identifisere, beskytte, oppdage, respondere og gjenopprette. I kjernen skal det identifiseres underliggende kategorier og disse skal sammenstilles med gjeldende informative referanser (standarder, retningslinjer, beste praksis) [39].

Rammeverkets nivåer (Tiers) skal fremme organisasjonens holdninger angående risiko knyttet til cybersikkerhet, og hvordan redusere den tilhørende risikoen. Nivåene skal beskrive hvilken grad organisasjonen praktiserer risikostyringen som er definert i rammeverket. Graden er ifølge rammeverkets nivåer delt inn i fire kategorier: delvis (nivå 1), risiko informert (nivå 2), repeterbare (nivå 3) og adaptive (nivå 4). Nivåene skal reflektere en progresjon der organisasjoner går fra et mindre strukturert cybersikkerhetsarbeid til mer formelle strukturer, med strategier som baserer seg på gjeldende retningslinjer og standarder [39].

Rammeverkets profil (Profile) skal representere resultatet som er basert på behovene identifisert under rammeverkets kategorier og underkategorier til en organisasjon. Denne profilen kan karakteriseres som en sammenstilling av standarder, retningslinjer, beste praksis fra rammeverkets kjerne fremstilt i et gitt scenario. Profilen kan bli brukt til å detektere potensielle svakheter for å forbedre sikkerhetstilstanden ved å sammenligne den nåværende tilstanden med den ønskede tilstanden. Profilen utarbeides ved å bruke alle kartlagte kategorier, samt målsettingen og risikovurderingen til å vurdere hvilke risikoer som bør prioriteres. Den nåværende profilen kan også brukes til å understøtte beslutningen, samt til å beskrive progresjonen til å imøtekomme den ønskede profilen [39].

ENISA – Rammeverk for sikkerhet til statlige skyer

Rammeverket fra ENISA tilbyr veiledning for hvordan organisasjoner kan administrere statlige skyer på en sikker måte. Rammeverket tar for seg hele forløpet fra forkjøpsprosessen til en ferdigstilt skykontrakt. Fokuset i rammeverket er på hvilke steg en må foreta seg for å bevare sikkerheten og personvernet gjennom hele prosessen. Gjennomføringen av rammeverket er basert på en kjent metodikk kalt Deming syklus. Metodikken baserer seg på fire elementære aktiviteter som skal utføres kontinuerlig gjennom hele livsløpet til

organisasjonen. Det eksisterer i dag mange versjoner av den velkjente metodikken, men hensikten er den samme – kontinuerlig forbedring. En av de kjente versjonene er kalt PUKK-hjulet hvor de fire aktivitetene er *Planlegge*, *Utføre*, *Kontrollere* og *Korrigere*. For dette rammeverket er det brukt en slik tilnærming med noen tilpasninger innenfor de fire aktivitetene [40]:

1. *Planlegge*: Planleggingsfasen, fokuserer på policyer sammen med en strategi for å implementere sikringstiltak for å oppnå sikkerhetsmålene.
2. *Utføre*: Utføringsfasen involverer implementering og håndtering av sikringstiltak fra planleggingsfasen.
3. *Kontrollere*: Hovedmålet med kontrollfasen er å revidere samt evaluere om de implementerte tiltakene utførte sin tiltenkte funksjon ved å se på nytteverdien og effekten der hvor tiltakene ble gjort. Under kontrollfasen vil også tester og øvelser bli gjennomført for å kvalitetssikre tiltakene slik at de har best mulig utgangspunkt for å kunne fungere som tiltenkt og for å tilfredsstille sikkerhetsmålene.
4. *Korrigere*: I den siste fasen skal eventuelle kartlagte svakheter fra kontrollfasen følges opp, samt utbedres for å hindre sikkerhetshull i de implementerte tiltakene. I denne fasen blir også nye tiltak introdusert. De nye tiltakene skal deretter gjennomgå den samme prosessen på nytt, slik vil denne syklusen fortsette gjennom hele livsløpet.

Under hver fase i PUKK-hjulet er det delt inn flere underkategorier med varierende aktiviteter som er nødvendig for å kunne presisere behovene og kravene fra offentlige aktører. Som rammeverket tilsier, skal dette brukes i samvirke med andre retningslinjer og være en del av et større styringssystem for å bevare cybersikkerheten i organisasjonen [41].

ISO/IEC 27001 Ledelsessystemer for informasjonssikkerhet

ISO/IEC 27001 er en internasjonal standard for hvordan man kan utarbeide et styringssystem for å bevare informasjonssikkerheten. Standarden stiller krav om etablering, implementering, vedlikehold og kontinuerlig forbedring til et ledelsessystem for informasjonssikkerheten. Formålet til standarden er å kunne gjøre arbeidet med å beskytte sin informasjon mer effektivt og enklere å styre. Styringssystemet skal være en risikobasert tilnærming ved hjelp av den nevnte PUKK-metodikken. Ved å følge standarden vil man kunne oppnå en kontinuerlig arbeidsprosess som skal forbedre informasjonssikkerheten [42].

For å tilfredsstille standarden er organisasjoner nødt til å utarbeide informasjonssikkerhetspolicyer, sikkerhetsmål med tilhørende strategier. Videre må de ha en

dokumentert risikobasert tilnærming for å vurdere cybersikkerhetstilstanden, samt sine implementerte tiltak og planlagte tiltak. Deretter stiller standarden krav til hvordan man overvåker informasjonssikkerhetstilstanden ved å blant annet gjennomgå avvikshåndteringssystemet. Neste aktivitet er å måle effektiviteten på styringssystemet, dersom noen aktiviteter gjøres ineffektivt skal dette forbedres ved å iverksette sikringstiltak. Her må det også dokumenteres hvilke fokusområder målingene tar for seg og hvordan disse målingene skal gjennomføres. En metode for å gjennomføre målinger på er ved å gjennomføre en intern revisjon som også skal dokumenteres. Distribusjon av informasjonssikkerhetspolicyer i organisasjonen er essensielt for å bevare god sikkerhetskultur innad i organisasjonen. Standarden sier at kartlegging av kompetansebehov skal være en del av sikkerhetsarbeidet hvor en må påse at ansatte får den kompetansen teknologien krever. Til slutt vil også standarden at organisasjoner har kommunikasjonsprosedyrer som beskriver ansvarsfordelinger til hvordan kommunikasjonen skal foregå [42].

3.5 SIKKERHETSKULTUR

Sikkerhetskultur er et omfattende begrep, der selve betydningen av begrepet blir tolket ulikt. En tilnærming til sikkerhetskulturbegrepet som Bang (2013) brukte var «*de sett av felles normer, verdier og virkelighetsoppfatninger som utvikles i en organisasjon når medlemmene samhandler med hverandre og omgivelsene, og som kommer til uttrykk i medlemmenes handlinger og holdninger på jobben*» [43, p. 337]. Ifølge NorSIS sin rapport[7] fra 2018 kommer det frem at så mye som 71% ikke får opplæring om digital sikkerhetskultur basert på de to siste årene. I tillegg har NVEs rapport fra 2017 om informasjonssikkerhetstilstanden i energiforsyningen fremhevet at menneskelig feil og kunnskapsmangel er den ledende grunnen til uønskede hendelser [44]. Menneskelig feil er som rapporten konkluderer med, en av de største årsakene til at uønskede hendelser realiseres.

Cybersikkerhet har i stor grad vært preget av en naiv innstilling på at «dette skjer ikke meg», som kunne bidra til å skape en dårligere holdning med tanke på cybersikkerhet. Tall fra DSB sin rapport[8] viser dog at denne innstillingen er i ferd med å endre seg. Ifølge rapporten fra 2020 sier nesten 40% av befolkningen at de er bekymret for digitale angrep mot styringssystemer her i Norge, mens det er rundt 35% som fremdeles er mer bekymret for

[7] Malmedal, B. (2018) *Nordmenn og digital sikkerhetskultur, NorSIS*
[8] DSB (2020) *Befolkningsundersøkelse om norske husholdningers bevissthet og atferd knyttet til egenberedskap*

terrorangrep. Men til tross for at fokuset rundt cybersikkerhet har økt de siste årene, sier Mørketallsundersøkelsen[9] at hele 67% av bedriftene at årsaken til sikkerhetsbrudd var tilfeldigheter eller uflaks. Dette viser at det fortsatt er en større prosent som ikke har den rette innstillingen når det kommer til cybersikkerhet. Dette problemet blir enda tydeligere når det også kommer frem hvordan sikkerhetsbruddene ble oppdaget. Rapporten sier at halvparten av bedriftene ikke har et rammeverk for informasjonssikkerheten og at sikkerhetsbrudd har blitt oppdaget ved ren tilfeldighet [37].

Organisasjoner kan investere tid og ressurser i å implementere tekniske sikringstiltak for å beskytte seg mot digitale angrep. Eksempelvis kan virksomheter utarbeide systemer for adgangskontroll, men dette vil i realiteten ikke gjøre en organisasjon sikrere dersom det organisatoriske aspektet ikke gjenspeiler det teknologiske. Ifølge Reason (1997) kan en god sikkerhetskultur kjennetegnes slik [45]:

- Har meldesystemer som samler opp, analyserer og vurderer informasjon ifra uønskede hendelser.
- Har meldesystem med løpende tilsyn.
- Har meldekultur hvor ansatte rapporterer egne feil og uønskede hendelser.
- En kultur som oppfordrer og belønner rapportering, samtidig som det finnes grenser på hva som er tolererbart og ikke-tolererbart vedrørende oppførsel.
- Er fleksibel, i muligheten til endring av den organisatoriske strukturen i møte med vanskelige oppgaver.
- En vilje og evne til å ta kloke beslutninger på grunn av informasjon ifra rapporteringssystem, og kan iverksette reformer når det trengs.

Sikkerhetskulturen fokuserer i stor grad på menneskers holdninger til sikkerhet, og at det er dårlige holdninger og få organisatoriske sikringstiltak som fører til sikkerhetsbrudd. Teorien om Resilience Engineering belyser et annet perspektiv om menneskets kapabilitet, og hvordan nettopp mennesket kan være en nøkkelbrikke for å oppnå en god sikkerhetskultur.

3.5.1 Resilience Engineering

For at en organisasjon skal kunne oppdrive en sikkerhetskultur i paradigmeskiftet innen digitalisering krever dette en ny måte å tenke sikkerhet på. Teorien om Resilience

[9] Næringslivets sikkerhetsråd (2018) *Mørketallsundersøkelsen 2018, Opinion AS*

Engineering kan beskrive dette ved å omstille tankeprosessen som før ble brukt til å arbeide med sikkerhet. Tidligere var fokusområdet i stor grad på storulykker, menneskelige feilhandlinger, svikt i tekniske systemer og manglende oversikt i et komplekst system. Resiliens beskriver en egenskap et system har til å være motstandsdyktig under ytre påkjenninger. Det beskriver også hvordan et system kan raskt komme tilbake i normaltilstand ved en hendelse og begrepet er tett knyttet til redundans. Hollnagel et.al (2006) definerer resiliens som «*en iboende egenskap som gir mulighet til å opprettholde eller å gjenvinne en stabil tilstand og fortsette driften etter en uønsket hendelse eller under kontinuerlige, stressende påkjenninger* [46, p. 3].» Resilience Engineering går bort fra å kun basere seg på historiske data, men viser også til viktigheten av å være proaktiv, fremtidsrettet og tilpasningsdyktig. Fokusområdet til Resilience Engineering er utilsiktede uønskede hendelser i et sosio-teknisk system. Et sosio-teknisk systemet beskriver interaksjon mellom de sosiale og tekniske faktorene [47].

Enkelte sosio-tekniske systemer har også iboende egenskaper for systemulykker, ifølge Perrow (1984) sin teori om normalulykker. Egenskapene kompleksitet og kobling er i stor grad kjennetegnene for dagens digitale verdikjeder. Systemer med høy interaktiv kompleksitet vil i stor grad samhandle på en ikke-lineær måte. Hendelsesforløpet til systemer med lineær samhandling er oversiktlige, forståelige og forutsigbare. Mens tette koblinger i stor grad fører til at en liten komponentfeil raskt eskalerer, uten noen barrierer for å hindre hendelsesforløpet. Perrow argumenterer for at systemer som kjennetegnes som høy interaktiv kompleksitet bare kan styres på en desentralisert måte, mens systemer for tette koblinger bare kan styres på en sentralisert måte. Digitale verdikjeder som kjennetegnes for både å være kompleks og tett koplet vil dermed ikke kunne styres i praksis, og er definisjonen på det systemet Perrow mener har større sannsynlighet for å bli utsatt for en normalulykke [48]. Ifølge Perrow er det fire strategier for å løse denne problemstillingen på [48]:

1. Reduksjon i interaktive kompleksitet for de komplekse systemene
2. Løsne opp koblinger i systemer med tette koblinger
3. En desentralisert organisasjon hvor den dominerende faktoren er interaktiv kompleksitet
4. En sentralisert organisasjon hvor den dominerende faktoren er tett koplede systemer

Et kjent sitat er at en aldri blir sterkere enn sitt svakeste ledd, og i et cybersikkerhetsperspektiv vil det alltid være mennesket som er det svakeste leddet. Denne

tilnærmingen har Resilience Engineering teorien derimot utfordret ved å presentere det i to systemer: medgjørlig *(tractable)* og ikke-medgjørlig *(intractable)* systemer. Et medgjørlig system kjennetegnes ved at de kan bli forstått i sin helhet. Systemet er stabilt og alle komponenter har simple beskrivelser om komponentens tilknytning. Ikke-medgjørlig system er motpolen til medgjørlig. De beskriver et system som uforståelig hvor det er utfordrende å følge prosessen, og alle involverte komponenter er vanskelig å detektere. Det er innenfor de ikke-medgjørlige systemene at mennesket har evnen til å påvirke utfallet dersom svikt skulle oppstå. Teorien kaller denne evnen for *ytelsesvariasjon*, og det beskriver menneskets tilpasningsdyktighet i en dynamisk situasjon som til sammenligning ikke en maskin kan ha dersom den ikke har tilgang til historiske datalignende hendelser [46, p. 128]. Man finner de ikke-medgjørlige systemene i sosio-tekniske system, der det foreligger utilstrekkelig informasjon om hvordan systemet fungerer. Menneskets vurderingsevne er essensielt i de systemer som ikke lett forstås, hvor prosedyrer ikke foreligger, og beslutninger må tas på stedet. Derfor vil menneskets kapabilitet også være en viktig suksessfaktor for å oppnå en god sikkerhetskultur i dette paradigmeskiftet som krever rask omstilling og fremtidsrettet nytenkning [46].

Prinsippene fra Resilience Engingeering kan sammenlignes med NSMs grunnprinsipper, Schiefloes modell for samfunnssikkerhet og Reasons kjennetegn ved en god sikkerhetskultur [49]:

- Læring – ta lærdom for å generere mer kunnskap, og utvikle seg ved å gjennomføre analyser og øvelser.
- Respondere – rask respons på uforutsette situasjoner, det å vite hvordan situasjonen kan utvikle seg og kunne håndtere en dynamisk situasjon.
- Overvåke – tidlig deteksjon av sikkerhetsbrudd oppnås ved kontinuerlig overvåkning.
- Forutse – proaktivt sikkerhetsarbeid skal kunne avdekke potensielle hendelser som kan føre til en uønsket hendelse.

Selv om mye peker på at mennesket er den utløsende årsaken til sikkerhetsbrudd, har også mennesket en avgjørende vurderingsevne til å påvirke situasjonen, ifølge denne teorien. Til tross for at systemer blir mer autonome og smarte, så er den menneskelige vurderingsevne og ytelsesvariasjon uerstattelig.

4 KAPITTEL: METODE

Metodekapitlet beskriver progresjonsprosessen til studiet. Riktig tilnærming og valg av metode er helt sentralt for å svare på problemstillingen, og tilhørende forskningsspørsmål. Utformingen av problemstillingen setter utgangpunkt for de metodiske og faglige beslutningene som foretas underveis i forskningsprosessen. Innsamling av data har i stor grad vært styrt av en kvalitativ tilnærming. Hvor det videre i dette kapittelet skal begrunnes, og forklares for valg som er gjort og hvorfor de er gjort. En kvalitativ tilnærming genererer informasjon om et tema hvor det eksisterer lite til ingen informasjon, som er tilfellet i denne studien. Hensikten med å beskrive forskningsprosessen er for at andre skal kunne etterprøve metoden.

4.1 VALG AV FORSKNINGSDESIGN

Bakgrunnen for studiet har vært å undersøke hvordan implementering av nye digitale målere i måleinfrastrukturen, samt skyløsninger vil påvirke den digitale og skybaserte verdikjeden hos NVE. Valg av forskningsdesign blir i all hovedsak styrt etter problemstillingens og forskningsspørsmålenes omfang. Prosessen for å besvare dette blir kalt for en forskningsstrategi, og er en prosess som skal kombinere forskningsspørsmål, empiri og konklusjonen for å besvare problemstillingen. Studiets problemstilling er følgende:

Hvordan kan NVE sikre den digitale og skybaserte måleverdikjeden for fjellskredvarling?

Fagfeltet cybersikkerhet har et hårfint skille mellom åpenhet og konfidensielt. Derfor måtte tilnærmingen av studiet kunne bli endret slik at det fortsatt var mulig å gjennomføre uten at det kom i konflikt med taushetsbelagte og sikkerhetsgradert informasjon. Tjora (2012) kaller denne tilnærmingen for et eksplorativt design. Det er et fleksibelt design godt tilpasset et fenomen som ikke har vært forsket på eller hvor tilstrekkelig informasjon ikke foreligger. Det eksplorative designet ble i den innledende fasen av arbeidet med studiet påvirket av en allerede etablert teori om risikostyring, cybersikkerhet, sikkerhetskultur og Resilience Engineering. I tillegg ble dokumentanalyser og intervjuer påvirket av at det skulle gjennomføres en grovanalyse. Grovanalysen var bakgrunnen for utformingen av spørsmålene til intervjuguidene, og styrte hvilken informasjon som ble innhentet av dokumentanalysen. Den metodiske tilnærmingen anvendt kalles for abduksjon og er en mellomting av induksjon og deduksjon. Ved å anvende en abduksjon kan man ut ifra empiri og teori besvare problemstillingen. Studiet vil da kunne bli styrt av informasjon som kommer fra datainnsamlingen. Denne metodikken er forklart av Tjora (2012) som sier at den abduktive

tilnærming starter med empirien. Dette vil påvirke innholdet i teorien og andre perspektiver som kan være hjelpsom for å se nytten og innholdet av den innsamlede dataen. Bakgrunnen for å velge den abduktive tilnærmingen har vært å kunne styre unna informasjon som kunne føre til skjermingsverdig informasjon, noe som kunne gjort det vanskeligere å gjennomføre grovanalysen [50].

4.2 KVALITATIV FORSKNINGSMETODE

Cybersikkerhet og digitaliseringen har blitt mye forsket på de siste årene, til tross for at det er relativt nye fenomen. Den økende oppmerksomheten rundt cybersikkerhet og digitaliseringen har ført til at det i dag eksistere en rekke dokumenter som kan være nyttig å studere nærmere. Det eksisterer dog lite til ingen informasjon om cybersikkerhet i kontekst av skredvarsling, så intervju måtte supplere der dokumentanalysen ikke var tilstrekkelig. For å kunne gjennomføre en grovanalyse var det ansett som mest hensiktsmessig å anvende kvalitative metoder. Grovanalysen er derfor bakgrunnen for valget av en kvalitativ forskningsmetode.

Den kvalitative metoden dokumentanalyse ble valgt for å utarbeide en grovanalyse etter standarden ISO 31000, men også bidra til den objektive risikoen som skal måles i form av sannsynlighet og konsekvens. Utarbeidelse av sannsynlighet og konsekvens sett i kontekst av en cyberhendelse er utfordrende å kvantifisere, men ved hjelp av ekspertkunnskap er det mulig å tilegne seg slik informasjon. Bakgrunnen for valget av å benytte seg av ekspertkunnskap ligger også i gjennomføringen av grovanalysen. Uten slik informasjon vil det være vanskelig å framstille risikoen ved hjelp av risikomatriser vedlagt. Funnene fra de kvalitative metodene er utgangspunktet for innholdet i grovanalysen.

For å tydeliggjøre hvilke fremgangsmetoder som er anvendt for å besvare problemstillingen, samt forskningsspørsmålene er det valgt å illustrere dette ved hjelp av tabellen 4.2.1 I dokumentanalysen henviser den til et dokumentnummer, forklaring til dokumentnummeret ligger vedlagt.

Metode / **Problemstilling/ Forskningsspørsmål**	**Dokumentanalyse**	**Semi-strukturert dybdeintervju**

Hvordan kan NVE sikre den digitale og skybaserte måleverdikjeden for fjellskredvarsling?	Dok.nr: 1.1, 1.3, 1.4, 2.2, 2.3, 2.4, 2.5, 2.6, 3.1, 3.2, 3.3, 3.4	Informanter med kunnskap om sikringstiltak, skyløsning og måleinfrastruktur for skredvarsling
i. Hvordan ser risikobildet ut for måleverdikjeden skredvarsling, og hva er den største risikoen?	Dok.nr: 2.1, 2.2, 2.3, 2.7	Informanter med kunnskap om cybersikkerhet
i. Hvordan kan man redusere sårbarheten, samt bevare integriteten og tilgjengeligheten ved bruk av digitale målere og skybasert løsning?	Dok.nr:1.1, 1.2, 1.4, 2.2, 2.4, 2.5, 2.7, 3.3, 3.4	Informanter med kunnskap om sårbarhet, skyløsning og måleinfrastruktur3 for skredvarsling
ii. Hvordan kan en styrke evnen til å beskytte seg mot ytre påkjenninger i den digitale måleverdikjeden?	Dok.nr:1.4, 2.2, 2.6, 2.4,	Informanter med kunnskap om sikkerhetskultur, cybersikkerhet og nåværende sikkerhetsnivå

Tabell 4.2.1 Matrise som viser anvendt metode på problemstilling og forskningsspørsmål

4.3 DOKUMENTANALYSE

En viktig del av datainnsamlingen for studiet har vært å ta utgangspunkt i eksisterende rapporter, standard, rammeverk og interne dokumenter som skal gi et grunnlag for grovanalysens metodiske gjennomføring. Dokumentanalysen gir også utgangspunkt for de første intervjuguidene som ble utarbeidet. Fordeler ved å benytte dokumenter er at innsamlet data er etablert uavhengig av studiets medvirkning, og at den derfor ikke vil bli påvirket som følge av datainnsamlingen. Dokumenter er i stor grad tilgjengelig og har ingen etiske begrensinger [51]. Ifølge Thagaard (2011) er studie av dokumenter ofte et godt supplement til metoden intervju.

4.3.1 UTVELGELSE AV DOKUMENTER

En stor utfordring knyttet til dokumentstudier er omfanget av informasjon som er tilgjengelig. Derfor var det i startfasen av studiet viktig å avklare sammen med NVE hvilket system grovanalysen skulle ta for seg. I tillegg definere hva som var innenfor og utenfor kontekst, slik at søkene kunne avgrenses i oppstartsfasen. Tilsendte rapporter fra NVE og konkret veiledning vært en betydelig faktor i utvelgelsen av relevante rapporter og rammeverk. Formålet med dokumentanalysen var å kunne skape en helhetlig forståelse av NVEs skredvarslingssystem. Dokumentene som er anvendt i studiet kan deles inn i tre overordnede kategorier:

Standarder og regelverk er nødvendig for å kunne gjennomføre en grovanalyse som baserer seg på en standard med gitte retningslinjer. ISO-standard har gitt grunnlaget for hvordan gjennomføringen av grovanalysen har vært. Byggteknisk forskrift (TEK 17) har vært viktig for å vise til kritikaliteten av operativ overvåkning av risikoutsatte fjellparti.

Rapporter og trusselvurderinger gir informasjon om samfunnets trusselbilde med aktuelle trender innenfor det digitale domenet som man kan forvente å se mer eller mindre av i nær fremtid, samt hvilke utfordringer samfunnet står ovenfor i dag. Trusselvurderingene fra PST, E-tjenesten, NSM og DSB har vært viktige dokumenter for empirien og analysen.

Interne dokumenter har vært nødvendig for gjennomføringen av grovanalysen. Interne dokumenter tilsendt fra informanter har vært nødvendig for å kunne beskrive et system som ikke kunne la seg forstås uten illustrasjoner. Interne dokumenter har også blitt brukt som veiledningen for risikoakseptkriterier, til å måle en objektiv risiko og utvelgelse av sannsynlighet, samt konsekvens.

4.4 SEMI-STRUKTURERT DYBDEINTERVJU

Intervjuene skulle supplere dokumentanalysen der informasjonen ikke var tilstrekkelig nok. Intervjuene ga videre informasjon for hvilke problemstillinger som burde bli undersøkt i dybden. De første intervjuene ga deretter grunnlag for videre prosess med valg av informanter og spørsmål. Intervjuguidene ble derfor utarbeidete ved å benytte den abduktive tilnærmingen. Hvor data fra de første intervjuene la grunnlaget for utarbeidelsen til de nye intervjuguider. Bakgrunnen for å kontinuerlig endre intervjuguiden er for å få et detaljert og helhetlig bilde som gir et dekkende grunnlag for å grovanalysen [50].

Intervju er en kvalitativ metode som brukes fordi en person med rett kompetanse og erfaring er en god kilde til informasjon. Et intervju kan gjennomføres på ulike måter, og måten som ble brukt i dette studiet var et semi-strukturert dybdeintervju. Formålet med et semi-strukturert dybdeintervju er å skap en relativ fri samtale som omgår noen spesifikke temaer som var forhåndsutvalgt. En slik fleksibel tilnærming vil kunne oppnå innsyn i informantenes refleksjoner rundt temaet, samt egne erfaringer og meninger. For grovanalysen var det nødvendig med informasjon fra personer som sitter med rett kompetanse. De vil bidra med ekspertkunnskap som kan brukes til å vurdere hvordan implementeringen av digitale målere og skytjeneste vil bli [52].

4.4.1 UTVALG AV INFORMANTER

Valg av informanter er et avgjørende valg man gjør som kan påvirke sluttresultatet. Nøkkelpersonell kan bli definert som en informant som besitter helt sentral informasjon som kun er kjent for den aktuelle informanten, og ansett som verdifull informasjon. Det er derfor viktig å finne rett nøkkelpersonell for å svare på spørsmål relatert til problemstillingen. Antall informanter må også være en del av vurderingskriteriet for å kunne skape en breddeforståelse gjennom verdikjeden [52].

Ifølge Njå et.al (1998) skal man i utvelgelse av eksperter basere seg på hovedprinsippene kredibilitet, likevekter og apriori forberedelser. Prinsippet kredibilitet tar utgangspunkt i at ekspertens beste evaluering er presentert. Kredibilitet til eksperter kan sikres ved å vite hvilken bakgrunn informantene har som gjør at informanten har de beste forutsetningene for å gi de svarene en ønsker. Likevekter baserer seg på at ekspertuttalelser fra forskjellige eksperter skal veie like mye. For å forsikre likevekt fra eksperter ble det valgt å gjennomføre til sammen åtte intervju, hvor alle hadde like forutsetninger og med varierende bakgrunn. Apriori forberedelse er den nødvendige forberedelsen som må gjøres for å utnytte tiden til eksperten på en optimal og ressurseffektiv måte [53]. Apriori forberedelse ble gjort i form av å sende intervjuguiden som skulle bli brukt under intervjuet på forhånd slik at ekspertene kunne forbedrede seg, og dermed sikre effektivitet under gjennomførelsen av intervjuet.

Grovanalysen var den avgjørende faktoren som styrte prosessen for utvelgelse av ulike informanter. Basert på valget om å begrense til systemet for skredvarsling og implementering av ny teknologi ble det nødvendig å se på flere informanter langs den digitale verdikjeden. NVE kunne bistå med informasjon om hvilke informanter det var relevant å kontakt for å avtale tidspunkt for gjennomføring av intervju. Informantene i denne studien har vært nøkkelpersonell som besitter informasjon om viktige elementer for skredvarslingstjenesten, cybersikkerhet og datasystemer. Variasjonen i bakgrunn og erfaring fra informantene skaper en breddeforståelse innenfor cybersikkerhetstilstanden i måleverdikjeden. Denne variasjonen var også nødvendig for å sikre likevekt i ekspertkunnskapen som kunne brukes i grovanalysen. Alle informantene hadde ansvarsroller innenfor sitt fagfelt, og hadde kunnskap eller erfaring til å kunne svare på spørsmål angående cybersikkerhet. Grovanalysen krevde også fagkunnskap fra flere ledd av den digitale verdikjeden til å vurdere hendelsesforløpet til en uønsket hendelse. Dette ble tilfredsstilt ved å velge informanter som hadde ansvar for

overvåkingssenteret, samt informanter med ansvar på NVEs hovedkvarter. Av hensyn til personvern og sporbarhet vil ikke ytterligere stillingsbeskrivelse eller ansvarsroller defineres tydeligere enn definert i tabell 4.4.1.

Informanter	**Ansvarsområde**
Informant A	Overvåkingssentret - Stranda
Informant B	Overvåkingssenteret - Kåfjord
Informant C	Reguleringsmyndigheten for energi (RME) - Oslo
Informant D	Tilsyn og beredskap - Oslo
Informant E	Drift og brukerstøtte - Oslo
Informant F	IT-Drift - Oslo
Informant G	Systemutvikling - Oslo
Informant H	Systemansvar for arkiv - Oslo

Tabell 4.4.1 Oversikt over informanter med tilhørende ansvarsområde

4.4.2 FORBEREDELSER OG GJENNOMFØRING AV INTERVJUENE

For denne studien ble det utarbeidet tre intervjuguider, disse ligger vedlagt. Intervjuguidene var tilpasset informantenes fagområde, ut ifra dokumentanalysen og grovanalysen. Det første intervjuet skulle gi en mer generell informasjon om måleinfrastrukturen, og cybersikkerhet som kunne brukes til å spisse de andre intervjuguidene ytterligere. Andre intervjuguide ble utarbeidet med hovedfokus på måleinfrastrukturen for å kunne følge opp informasjon fra første intervju. Tredje intervjuguide sitt hovedfokus var cybersikkerheten, samt tilhørende sårbarheter. Den tredje intervjuguiden ble noe tilpasset for informantenes fagområde, men hadde flere gjentakende spørsmål for å samle bred kunnskap til grovanalysen. Oppbyggingen til intervjuguiden fulgte en semi-strukturert strategi for å kunne gi rom for tilleggsspørsmål underveis dersom informasjonen skulle ha behov for ytterligere utdyping og avklaring. Semi-strukturerte intervju skaper en åpen atmosfære der samtalen ikke lar seg bli fullstendig styrende av guiden [51].

Intervjuguiden ble i forkant av alle intervju tilsendt intervjuobjektene, slik at forberedelser kunne føre til en mer effektiv og kvalitetssikre gjennomgangen i henhold til en apriori forberedelse. Informantene ble introdusert for studiet av biveileder, med unntak av to informanter som ble introdusert muntlig i forkant av intervjuet. Grunnet COVID-19 ble det besluttet å gjennomføre intervjuene via en digital plattform. Den digitale plattformen som ble benyttet var Microsoft Teams. Bakgrunnen for dette valget er kun basert på tilgjengelighet

uten andre hensyn tatt i betraktning. Dette skal ikke ha påvirket resultatene eller informantenes åpenhet, i forhold til at innhentet informasjonen ikke var sensitive. Intervjuene ble gjennomført i perioden mars-mai. Bakgrunnen til at intervjuene ble strekt over et såpass langt tidsrom er noe grunnet COVID-19, men også fordi det er et krevende tema som må undersøkes og at en trenger tid til å prosessere og forstå dataen. I tillegg så dukket det opp flere spørsmål underveis i arbeidet med grovanalysen som gjorde det nødvendig å gjennomføre flere intervju. Intervjuene hadde en varighet fra 1 til 2 timer, hvor det under hele intervju ble tatt notater. Ved en anledning ble det brukt opptak med informantens samtykke. Transkribering er en tidkrevende prosess som i noen tilfeller kan være bortkastet, så en transkribering uteble for de resterende intervjuene. Dette valget ble besluttet i samråd med veileder, som heller anbefalte å stille eventuelle oppfølgingsspørsmål på mail for å kvalitetssikre at informasjon notert var gyldig tolket. I tillegg var det nødvendig med interne dokumenter for å skjønne måleinfrastrukturen i den digitale verdikjeden, som var vanskelig å forklare muntlig uten tegninger. Disse dokumentene er ikke vedlagt grunnet noen sensitive opplysninger.

4.5 STUDIENS KVALITET

Frem til nå er det redegjort for valgene som er tatt for å besvare problemstillingen. Når en foretar et valg er det også noe man velger bort av ulike grunner, derfor vil det være nødvendig å se på fordeler og begrensninger til metodene en har valgt slik at dette blir hensyntatt.
Fordi dette er en kvalitativ studie blir begrepene troverdighet, gyldighet, overførbarhet og usikkerhet brukt til å beskrive studiens kvalitet [51]. Hvor troverdighet betyr hvilken tillit man har til utførelsen av forskningen. Begrepet gyldighet er tilknyttet tolkningens kvalitet som gjøres underveis, og om det finnes andre typer forskning som kan underbygge den tolkningen. For overførbarhet vil det bety i hvilken grad kan resultater fra denne forskningen også være legitime i andre settinger. Usikkerhet blir i denne studien brukt som et mål på den gyldigheten og troverdigheten til resultatene for grovanalysen.

4.5.1 TROVERDIGHET

Reliabilitet kan forstås som forskningens troverdighet. Troverdigheten kan bli begrunnet med å argumentere for hvordan dataen blir trukket ut i løpet av forskningsprosessen. Forskningen kan påvirke både de som blir undersøkt og de som undersøker fordi det er mennesker som forholder seg til hverandre. Uoppmerksomhet eller slurv kan påvirke forskningsprosessen og kompromittere troverdigheten til dataen som er innhentet. Derfor er det viktig å være bevisst

på denne potensielle fallgruven ved å være tydelig i språket og skjerpet under innhenting av data og i analysen. Metodekapittelet skal være den delen av forskningsprosessen hvor valg og beslutninger blir synliggjort for å øke bevisstheten rundt eventuelle faktorer som kunne ha påvirket utfallet av studiet [51]. Troverdigheten blir tatt hensyn til ved å presentere data, metode og beskrive avgjørelsene. En del av prosessen er å drøfte hvordan presentasjon av data skal se ut for å bekrefte samsvaret mellom problemstillingen og innhentet material.

Intervjuguiden var av en semi-strukturert oppbygning med åpne spørsmål for å gjøre rom for oppfølgingsspørsmål. Åpne spørsmål vil forsikre mer autentiske svar, heller enn ledende spørsmål som fører til en forventning eller begrenser informantens svaralternativ [54]. Dette førte til noe variasjon av spørsmålene, fordi intervjuguiden ble som nevnt tilpasset noe til fagområdet til informanten. Dette gjorde også at noen spørsmål uteble da informant ikke hadde rett forutsetning for å svare. Men en intervjuguide er med på å øke troverdigheten fordi gjennomføringsmetoden var lik for alle informantene. I empiri er det redegjort for hva som er informantenes subjektive meninger. Som et supplement til empiri har også dokumentanalysen virket som en objektiv bidragsyter, noe som styrker troverdigheten til forskningsdataen.

Cybersikkerhet er som nevnt tidligere et utfordrende tema å snakke om med tanke på bedriftssensitiv informasjon. Dette kan ha ført til noe overfladiske svar, eller svar som ikke direkte kan knyttes opp mot studiets problemstilling fordi det kan være av sensitive opplysninger. Informantene har likevel klart å gi utfyllende svar
rundt sine erfaringer og subjektive meninger om hvordan håndtering av cybersikkerhet oppleves uten å utlevere sensitiv informasjon.

4.5.2 GYLDIGHET

Gyldighet kan vurderes ut fra om tolkningene og resultatene som fremkommer er legitime, sammenlignet med den virkeligheten som er studert [51]. For å bevare gyldigheten til forskningen er det valgt å benytte metodetriangulering. Metodetriangulering handler om hvordan et fenomen kan undersøkes fra minst to ulike perspektiver [51]. De to ulike perspektivene i studiet har vært basert på hvor informantene befinner seg i den digitale verdikjeden. To av informanter befant seg på den ytterste delen, men de seks resterende befant seg i midten av den digitale verdikjeden. Dette vil styrke studiets gyldighet ved at informanter representerer to ulike ledd av den digitale verdikjeden, og underbygger innholdet i grovanalysens resultat. Videre argumentasjon for forskningens gyldighet er at alle

informanter hadde kompetanse og et sentralt ansvarsområde innenfor cybersikkerhet. I tillegg har dokumentenes validitet blitt bevart ved å ta i bruk offentlige dokumenter fra legitime kilder som NSM, DSB, E-tjenesten og PST. Informasjon hentet ut fra dokumentene kan derfor med stor grad av sikkerhet regnes som legitime. En potensiell fallgruve som man må være observant på er at informasjon som er generert fra dokumentene er egne tolkninger av tekstdata, noe som kan ha påvirket forskningen [54]. Denne fallgruven har man vært klar over og prøvd å begrense ved å være bevisst over valg av dokumenter, samt diskutere tolkningene med veileder. I tillegg har man ved å være konsekvent med kildehenvisning også mulighet til å spore tilbake til informasjonen fra dokumentene. En annen begrensing til gyldigheten for forskningen er den manglende informasjonen og historisk data som finnes på cybersikkerhet i kontekst av skredvarsling. Dette gjorde at dokumentanalysen ikke kunne bekrefte eller avkrefte funn som kom frem fra intervjuene. For å kompensere for manglende dokumentasjon ble det heller valgt å intervjue åtte informanter som kunne sette cybersikkerhet i kontekst av skredvarsling.

Videre har gyldigheten blitt bevart ved å benytte den abduktive tilnærmingen til utarbeidelsen av intervjuguider. Informantenes uttalelser kunne sådan bli etterprøvd ved å teste hvorvidt andre informanter kjente seg igjen i den samme uttalelsen eller ikke. I tillegg så har forskningsdata, mer spesifikt utarbeidelsen av den digitale verdikjeden, blitt utarbeidet i samarbeid med informant A. I etterkant ble den digitale verdikjeden også forklart for informant B, med samme bakgrunn som informant A, som deretter kunne verifisere innholdet. På bakgrunn av viktigheten av leddene i den digitale verdikjeden, og dets betydning for grovanalysen var dette ansett som nødvendig. En potensiell begrensing er at informanter fra de eksterne leverandørene ikke fikk mulighet til å si sin side av saken. Informanter fra leverandører og underleverandører kunne vært inkludert for å ytterligere kvalitetssikre forskningsdata.

4.5.3 Overførbarhet

Ifølge Tjora (2012) er målet med forskningsprosesser at de skal både være mulige å generalisere, samt være overførbare. Faktorer som påvirker generalisering og overførbarhet er studiets kontekst og tilhørende avgrensinger. Studiet er avgrenset til å kun se på den kritiske måleverdikjeden for skredvarsling. Det la følgelig begrensninger for utvalget av informanter som måtte være i måleverdikjeden. Metodikken grovanalysen som er benyttet for å utvikle gode sikringstiltak er overførbare i form av at det er en kjent metodikk som kan tilpasses

enhver sektor og virksomhet. Overførbarheten er i stor grad bevart ved å henvise til gitte rammeverk som er utgangspunktet for utarbeidelsen av grovanalysen. Funn fra risikobildet er også generaliserbart fordi det kan også være relevant for andre virksomheter i Norge. Det vil derimot ikke alltid være samsvar i hvordan en uønsket hendelse vil forvitre seg i virksomheten da alle virksomheter har ulike forutsetninger for å håndtere cybersikkerhet.

4.5.4 USIKKERHET

Risikoanalysemetodikken for studiet er en grovanalyse som er godt skikket tidlig i prosjektfasen som digitaliseringsprosessen til NVE. Men det å gjennomføre en grovanalyse for et komplekst og uoversiktlig system for måleverdikjeden for fjellskredvarsling er utforende. Derfor er det nødvendig å presentere alle usikkerhetsmomentene som er knyttet til grovanalysemetodikken. Usikkerhet kan deles inn i to kategorier; aleatorisk og epistemisk usikkerhet. Aleatorisk usikkerhet handler om en iboende usikkerhet og kan knyttes opp mot hendelser som vindstyrke, nedbørsmengde og skyldes naturlig variasjon. Denne usikkerheten kan ikke reduseres, men kan synliggjøres ved hjelp av normalfordeling. Epistemisk usikkerhet er knyttet til mangel på kunnskap, og kan ved å generere mer kunnskap bli redusert [35]. Når man gjennomfører grovanalyse vil det alltid være en form for usikkerhet, enten det er epistemisk eller aleatorisk. Det er derfor viktig å være klar over hvilke faktorer som kan påvirke usikkerheten til grovanalysen, og ved å være bevisst på usikkerheten kan man ta dette med i betraktningen. For grovanalysen vedlagt er det viktig å vite at det knyttes usikkerhet til følgende elementer [35]:

- Alle uønskede hendelser blir ikke identifisert – for den digitale måleverdikjeden vil det naturligvis ikke være mulig å identifisere alle uønskede hendelser. Dette utgjør derfor en usikkerhet for om risikonivået er akseptabelt.
- Modellusikkerhet – den utvalgte metodikken for å gjennomføre risikoanalysen vil i stor grad påvirke resultatet, og skikketheten på hvorvidt valgt risikoanalyse tilfredsstiller behovene til å oppnå forsvarlig sikkerhetsnivå. Grovanalysen er ikke på detaljnivå, noe som kan påvirke utfallet av analysen.
- Parameterusikkerhet – parameterusikkerhet er den usikkerheten knyttet til dataen brukt i analysen. Fordi data kommer fra informanter, og er subjektivt tolket vil det kunne knyttes usikkerhet i hvorvidt de er gyldige i henhold til det som står i grovanalysen.
- Konsekvensusikkerhet – for grovanalysen knyttes det stor usikkerhet for konsekvensvurderingen da det er manglende kunnskap rundt dette. Det finnes for lite

data på hvor mye skade blant annet en innsider kan gjøre, eller hva som blir konsekvensen av en potensiell feil i tilgangsstyringen for skyløsningen.

- Beregningsusikkerhet – det å måle risikoen som en objektiv størrelse er en usikkerhet i seg selv. Den beregnede risikoen tar utgangspunkt i en større risiko, enn hva som gjenspeiler virkeligheten. Dette kan påvirke hvordan man prioriterer sikringstiltak. Man kan risikere å implementere kostbare sikringstiltak for en uønsket hendelse som i realiteten går under akseptabel.
- Usikkerhet som følge av kort tidsramme – manglende tid til gjennomføring vil naturligvis føre til at potensielt viktige momenter av analysen ikke kommer frem. For denne analysen kunne ikke alle leverandører og underleverandører inkluderes da det ikke lot seg gjennomføre for den korte tidsrammen til studiet.
- Usikkerhet på grunn av manglende kompetanse – egen kunnskap og kompetanse til å vurdere og tolke data utgjør en betydelig del av usikkerheten. Derfor har alle antakelser gjort i grovanalysen blitt skriftlig vurdert og vedlagt i oppgaven.

5 KAPITTEL: EMPIRI OG RESULTATER

Dette kapittelet skal presentere funn gjort fra datainnsamlingen og risikoanalysen. Resultatene er basert på ekspertvurderinger fra informantene, funn fra dokumentanalysen og funnene som fremkommer av risikoanalysen vedlagt til å svare på problemstillingen. Kapittelet deles inn i to deler; del 1 tar for seg datainnsamling fra informanter og dokumentanalysen, og i del 2 vil resultater fra risikoanalysen bli presentert. Fra intervjuene blir informantenes ulike holdninger, synspunkter og erfaringer sammenstilt til breddekunnskap om et tenkt scenario relatert til problemstillingen.

5.1 DEL 1- PRESENTASJON AV INTERVJUER OG DOKUMENTANALYSEN

De empiriske dataene skal fungere som et kunnskapshevende verktøy om et fenomen som ikke før har blitt undersøkt eller hvor det foreligger utilstrekkelige mengdedata. Datainnsamlingen fra informantene er brukt til å kunne forstå hvilke muligheter og problemstillinger som NVE kan møte når de skal implementere ny teknologi. Det er valgt å fokusere på teknologiimplementering i den digitale verdikjeden for skredvarslingstjenesten. Datainnsamlingen fra dokumentanalysen er brukt til å se hvordan andre statlige organ organiserer cybersikkerheten, samt se på hvordan risikobildet ser ut i samfunnet generelt.

5.1.1 DEN DIGITALE MÅLEVERDIKJEDEN FOR FJELLSKREDVARSLING

Digitalisering fører til en mer sammenkoblet og kompleks verden. Hvor teknologi knytter sammen stadig flere leverandører i en allerede uoversiktlig verdikjede. Digitale verdikjeder er i dag så komplekse og uoversiktlige at DSB har utarbeidet en rapport[10] for risikostyring i digitale verdikjeder. Nye avhengigheter og tjenesteutsettinger byr på utfordringer rundt kartlegging av risikobildet til virksomheter. DSB karakteriserer dagens digitale verdikjeder som komplekse, lite oversiktlige, tett koblede og transnasjonale. En betydelig trussel for slike verdikjeder er å lokalisere hvor feil kan oppstå, som kan føre til momentan svikt i andre samfunnskritiske tjenester, som for eksempel skredvarsling. Styringsprinsippet i DSB sin rapport er basert på den klassiske *NS-ISO 3100:2018 Risikostyring* tilnærmingen. Hensikten med risikostyring av digitale verdikjeder er å redusere risikoen for komplekse verdikjeder. Rapporten veileder virksomheter til å vite hvilken informasjon fra leverandører som er relevant å spørre om. Videre hjelper rapporten virksomheter med komplekse verdikjeder å holde en systematisk oversikt [22].

Trusselvurderingene som kommer fra NSM, E-tjenesten, DSB og PST viser til forventede trusselkilder mot samfunnet. I PST sin rapport[11] kommer det frem at en av de mest alvorlige truslene er digital kartlegging og sabotasje av kritisk infrastruktur. Videre sier rapporten at statlig etterretningsvirksomhet er forventet å rette sitt fokus mot politiske myndigheter, naturressurser og næringsliv, forsvar og beredskap, samt forskning og utvikling. Trusselaktørene av størst skadepotensial er, ifølge rapporten russisk, kinesisk og iransk etterretningsvirksomhet, men at det er flere potensielle trusselaktører som kan være interessert i å rette skade mot Norge. *«Norge har naturressurser av stor betydning for energiforsyningen til andre stater. Dette er en maktfaktor, derfor ønsker andre stater innsikt i norsk energisektor»* [29, p. 8].

Mellom informantene er det en felles konsensus i at den menneskelige faktoren utgjør en del av det risikobildet som vi ser i dag. Informant B opplyser at «*mennesket utgjør 20-50% av sikkerhetsbruddene som oppstår»*. Informant A vurderer at det er innsideren som den største trusselen for overvåkingssentret. Denne oppfatningen av menneskets kapabilitet er også vurdert forskjellig for informantene. Informant C sa at «*angrepene er så sofistikerte i dag at man nesten må være ekspert for å gjenkjenne en phishing mail, (...) hvor den eneste løsningen til dette problemet er å installere tekniske barrierer fordi mennesket på et eller annet*

[10] DSB (2020) *Risikostyring i digitale verdikjeder*
[11] PST (2020) *Nasjonal trusselvurdering*

tidspunkt kommer til å gjøre feil». Videre sier informant C at det fremdeles er mange som har for dårlige passord. Mennesker ønsker at jobben skal gjøres effektivt slik at snarveier oppstår som igjen kan innføre en sårbarhet til systemet. Samtidig blir det lagt vekt på viktigheten av kompetanse og erfaring fra mennesker hos informanter som har større tro på menneskets ytelsesvariasjon. Slik som informant D belyste; «*om man tar utgangspunkt i måledata så kan en geolog på bakgrunn av erfaringer, kunnskap og direkte observasjon si at måledataen ikke stemmer med virkeligheten dersom de skulle være kompromittert*». Man har også blitt flinkere på å detektere forsøk, og dermed iverksette tiltak for å redusere sannsynligheten for vellykkede angrep. Kompetansehevende kurs og mer informasjon om cybersikkerhet spiller en sentral rolle for det forebyggende arbeidet. En gjentakende setning fra samtlige informanter er faren ved å ikke forstå eller ha nok kunnskap om det systemet man anvender. Informant B understreker et større behov for IKT-sikkerhet regionalt for å kunne håndtere IKT-sikkerhet på en forsvarlig måte. Dette blir i dag ansett som en tilleggsoppgave for det arbeidet som utføres for overvåkingssenteret. Selv om en kan se en endring innen sikkerhetskulturen vil det, ifølge informant D, ta mange år før det ligger som en naturlig del av arbeidsoppgavene.

NVE opplever daglig at mange forsøker å komme seg inn til NVE sitt system. Tidligere har NVE blitt utsatt for et angrep av typen løsepengevirus, hvor konsekvensen av det førte til tap av data. Etter slike hendelser evaluerer de og finner årsaken, hvor sårbarheten i dette tilfellet var svake sikringstiltak. Implementering av tiltak blir gjort for å forhindre en slik hendelse igjen, sier informant F.

For informantene fra overvåkingssentrene (A og B) ligger den største risikoen på integriteten til måledata. Tap av måledata eller kompromittert måledata kan føre til alvorlige samfunnsmessige konsekvenser. Dette er for informantene A og B den største og mest alvorlige risikoen. Verdien av måledata kan som informant B beskriver slik: *«GPS-utstyr til flere 100.000 kr kan erstattes, mister man måledata vil det påvirke i betydelig grad analyser og beslutninger som tas på bakgrunn av måledataen.»* Måledata gir beslutningsgrunnlag for beredskapsnivå. Dersom dette blir kompromittert eller kommer på avveie vil det ha signifikante konsekvenser for både menneskers liv og kapabiliteten til overvåkingssenteret.

5.1.2 IMPLEMENTERING AV NY TEKNOLOGI OG SKYLØSNING

NSM skriver i sin rapport at implementering av ny teknologi og digitaliseringen er et *tveegget sverd,* noe som vil si at det kommer med fordeler og ulemper. Fordeler i form av det fordrer et nødvendig skifte inn mot mer effektivisering og optimalisering av ressursbruk. Men med fordelene kommer det også ulemper i form av nye sårbarheter til teknologi som man har blitt helt avhengige av å bruke [55]. 5G er en av de implementeringene som samfunnet nå står ovenfor, og ifølge PST sin rapport[12], kommer denne utviklingen ikke uten sikkerhetsmessige utfordringer. Rapporten legger vekt på at det vil være umulig å avdekke om de teknologiske komponentene og programvarene som styrer enhetene inneholder skjulte, ondsinnede funksjonaliteter som muliggjør spionasje, manipulasjon og sabotasje. NSM har også i sin rapport lagt vesentlig vekt på sikker implementering av teknologi, spesielt mot skyløsninger. Bakgrunnen for dette var, ifølge rapporten[13], fordi man ser en stor økning av virksomheter som benytter seg av denne tjenesten. I rapporten står det «*for å redusere risikoen ved tjeneste-utsetting må virksomhetene sørge for ikke å bli låst til én leverandør*» [55, p. 34].

Flere virksomheter velger å benytte skyløsninger for å imøtekomme teknologiutviklingen som samfunnet står ovenfor. De aller fleste av skyleverandørene har per dags dato ikke installasjoner på norsk territorium. Dette medfører en risiko fordi data lagres utenlands. Virksomheter må ha tillit til at skyleverandør oppbevarer data på en forsvarlig måte som er i henhold til virksomhetens krav. Før implementering av skyløsning må det alltid foreligge en risikovurdering som tar for seg blant annet hva som kan skje dersom krig skulle oppstå eller en leverandør blir kjøpt opp/slått konkurs. Risikoanalysen må også kartlegge hvilke samfunnskritiske funksjoner som kan bli påvirket ved å ta i bruk transnasjonale leverandører. Dersom skyleverandøren har eksisterende sårbarheter uten at virksomheten er klar over dette, vil virksomheten kunne arve de samme sårbarhetene ved å ta i bruk skyleverandørens tjenester. NSM har i sin rapport utarbeidet en huskeliste for sikker implementering av skyløsning [55]:

- Benytt Cloud native-plattformer og applikasjoner da de er mer åpne og interoperable enn tradisjonelle plattformer og applikasjoner
- Velg åpne produkter basert på åpne standarder, ikke velg leverandørspesifikke løsninger

[12] PST (2020) *Nasjonal trusselvurdering 2020*
[13] NSM (2020) *Risiko*

- Ikke implementer løsningen på en proprietær måte. Bevar produktenes interoperabilitet og evne til å flytte applikasjoner mellom ulike applikasjonsplattformer
- Ikke bind løsningen til et spesifikt fysisk sted. Datasenter er en modell, ikke et sted. Ha nødvendig smidighet til å kunne flytte løsningen mellom ulike fysiske datasentre og kanskje til og med til ulike offentlige skyer – alltid i henhold til behov gitt i systemets sikkerhetskonsept.

Behovet for mer digitale løsninger er ifølge informant F todelt; føringer fra staten som fordrer digitaliserte løsninger og fordi alt fremover kommer til å skje via skyen. Skyløsninger er en robust tjeneste som kan gjøre det mulig å behandle data på en helt ny måte. Behovet for å ta i bruk skyløsninger er også et resultat av hvordan digitaliseringen ellers i samfunnet påvirker NVE som statlig organ. Informant G legger frem at ved å ta i bruk digitaliserte løsninger vil man gi en mulighet til å sammenstille data fra kunder og andre aktører slik at man kan samarbeide på en helt ny måte. Videre sier informant G at det å kunne gjøre data mer tilgjengelig er en helt sentral årsak til å ta i bruk skyløsninger. Skytjenestene vil, ifølge informant G, gi rom for mer fleksibilitet og introduserer nye verktøy som kan tas i bruk for å håndtere store mengder data på en kostnadseffektiv måte. Samtidig gir det rom for mer fleksibilitet i den forstand at ansatte har mulighet til å kunne jobbe sammen til uavhengig av avstanden. Ifølge informant A ligger behovet utelukkende på egne ønsker om å effektivisere oppgavene sine, og et ønske om å ta i bruk ny teknologi. Teknologien som overvåkingssenteret benytter i dag krever mye vedlikehold og er svært strømavhengige for å kunne fungere optimalt, som de til enhver tid må. Derfor er ny teknologi, spesielt digitale målere, nevnt av informant A, som en svært interessant løsning på dagens måleinfrastruktur. «*Men sikkerheten må være helt framme i pannebrasken, og vi må være 100% sikker på den teknologien vi velger å bruke*», (Informant A).

Det brukes mye ressurser på analyser og vurdering om teknologien som skal tas i bruk. Azure er den skyløsning fra Microsoft som NVE nå prøver å implementere i sin daglige bruk. «*Fordi tjenester i datarommet går mot skyløsninger og ikke mot databaser er man nesten tvunget til å gå over til skyløsninger*», (Informant F). Bakgrunnen for valget av Azure var ifølge informant F fordi «*NVE er homogent i forhold til Microsoft og litt fordi det var lettvint*» så det var en enklere overgang ettersom de allerede hadde tjenester som Office 365. Valg av skyløsninger er, ifølge informant C, et kompromiss mellom ønskede kvalifikasjoner og hva

som er realistisk å gjennomføre. Det kan være at NVE har ønskede sikkerhetskrav til leverandøren, hvor dette ikke kan gjennomføres fra leverandøren. Ifølge informant C blir det i tilfellet med implementering av Azure en «*take it, or leave it*» situasjon som oppstår. Dette oppstår, ifølge informant C, som følge av at Microsoft allerede har en systemløsning for alle brukere av skytjenesten. Dersom sikkerhetskrav fra NVE påvirker denne systemløsning velger Microsoft som er en stor internasjonal aktør, å ikke tilpasse seg NVEs sikkerhetskrav. Dette fører til at det blir opp til NVE å sørge for at skytjenesten brukes etter NVEs sikkerhetskrav med gitte datadelingsgrensesnitt og egen systemløsning i Azure.

I vinter 2020 ble det gjennomført et pilotprosjekt på Azure, hvor konklusjonen var at per dags dato er NVEs måleverdikjede for fjellskred ikke klar for en ny systemløsning som kun baserer seg på skyløsning. Bakgrunnen for denne vurderingen ligger i overvåkingssentrenes krav fra TEK 17 til 24/7 overvåkning, hvor det å lagre data andre plasser enn lokalt er vurdert som for risikabelt. NVE går derfor videre med hybridløsning hvor deler av verdikjeden er tilknyttet Azure. Overvåkingssentrene derimot skal gå over til plattformen Splunk for å kunne lagre sine data lokalt. Splunk er en on-premises løsning for å sikre et lukket nettverk. Splunk Inc. er et amerikansk, multinasjonalt, offentlig selskap med base i San Francisco, California, som produserer programvare for å søke, overvåke og analysere maskingenererte big data via et datadelingsgrensesnitt [56]. Splunk er, ifølge informant B, en mer proaktiv løsning som kan analysere store datamengder, men kommer med en ulempe i form av at det krever god teknologikunnskap for å forstå Splunk. Informant B sier at «*implementeringen må derfor skje trinnvis hvor man på et tidspunkt blir stående med to systemer som er helt operativt*». Informant F understreker at økonomi er ikke et grunnlag for å gå over til å bruke skyløsninger. «*Man blir nødt til å drifte to systemer over en lengre periode for å forsikre en sømløs overgang til skytjenesten*» (informant F).

Informasjon kommer til å bli lagret på en annen måte, og dette medfører en totalendring i NVEs nåværende databehandling og rutiner. Ikke bare blir dataen lagret på en ny måte, men den blir også lagret utenfor NVEs kontor. Dette var, ifølge informant F, uproblematisk på bakgrunn av at NVE ikke besitter mye skjermingsverdig informasjon. Det er en felles oppfatning hos informantene at kunnskap må ligge i bunn før en eventuell implementering av ny teknologi. Det å kunne forstå og bruke teknologien på en trygg måte er helt sentralt. I tillegg må man vite hvilken kompetanse som behøves for å dekke nåværende og fremtidige behov.

NVE har et stort aldersspenn over sine ansatte, og informant G sier at de unge maser om å få ta i bruk ny teknologi noe som ikke gjelder for de eldre ansatte. Implementeringen av ny teknologi krever en ny teknologiforståelse og informant G sier at det er krevende å holde oversikt over alle mulighetene. Ansatte trenger oppfølgning i hvordan verdivurdering av skjermingsverdig informasjon skal gjøres. Informant G sier at implementering av digitale målere og skyløsninger fordrer en superbruker som kan bistå ansatte med denne overgangen. Begrepet superbrukere blir brukt til å beskrive en person som har spisskompetanse innen et fagfelt eller en type teknologi, og bistår andre med å forstå og bruke teknologien på en forsvarlig måte. Informant G sier at å vurdere skjermingsverdig informasjon er helt grunnleggende før man tar i bruk en skyløsning. Dette for å forhindre at informasjon som ikke skal bli tilgjengeliggjort blir det. Holdningene til ansatte når det gjelder implementering av ny teknologi, nye løsninger og strukturelle endringer er stort sett positive. Men det foreligger også en skepsis til hvordan det faktisk kommer til å bli når det hele skal implementeres. Flere informanter nevner blant annet en risiko knyttet til forståelse av deling av informasjon ved bruk av skyløsninger.

Fra NSMs grunnprinsipper for IKT-sikkerhet kommer det frem at digitaliseringen fører til en økning av kompleksitet, hvor det er flere verdier som blir offentliggjort, nettet blir mer usikkert og verdikjeder som blir så lange at det er vanskelig å holde en oversikt [12]. Denne observasjonen samsvarer med informantenes meninger. Informant D peker på at dette fordrer en mye bedre håndtering av verdikjeden enn det som eksisterer i dag. Det kan oppstå mange uforventede hendelser når man implementerer ny teknologi, dog sier informant E at de er flinke til å håndtere uforventede hendelser. For skyløsninger sier informant E at «*det kommer til å bli annerledes med sky, fordi man kan ikke bare trekke ut pluggen*». Informant G forteller at det å implementere ny teknologi som skytjeneste ikke kommer uten sårbarheter. Sårbarheten kommer fordi det er mange ansatte som jobber på tvers av sektorer, at det kommer til å bli en utfordring å få kommunikasjonen til å skje sømløst mellom sektorene og videre i måleverdikjeden.

5.1.3 SÅRBARHETER, RISIKOKARTLEGGING OG SIKKERHETSSTYRING

Ifølge NSMs rapport[14] kommer det frem at et stort antall virksomheter ikke hadde foretatt risikovurderinger for alle relevante risikoområder [55]. I tillegg ble ikke vedlikehold

[14] NSM (2020) *Risiko*

opprettholdt over tid, noe som kan føre til at implementerte sikringstiltak ikke får den ønskede effekten for å redusere risikoen. NSM sier også at mengden åpen data som myndigheter deler gjøre det mulig for en trusselaktør å sammenstille informasjon som i utgangspunktet er skjermingsverdig informasjon. Den offentlige informasjonen kan bli misbrukt til å blant annet planlegge en målrettet uønsket handling mot nøkkelpersonell eller virksomheten. NSM fordrer bedre avveiinger over hvor mye informasjon, og hvilken informasjon som offentliggjøres i forhold til de fordelene deling av informasjonen har [55]. Samtidig blir offentlige aktører oppfordret til å dele mer data for å sørge for bedre dataflyt på tvers av sektorer og tilrettelegge for innovasjon ved at flere får tilgang til og kan gjøre nytte av informasjonen. DIFI har utarbeidet en veileder for tilgjengeliggjøring av åpen data, men foreløpig ligger Norge langt etter på tilgjengeliggjøring av data da det antas at ca 10% av relevante datasett er tilgjengeliggjort [57].

NVE har en relativt offentlig deling av sine data, noe informant H mener burde vært mer begrenset. Det er spesielt kraftsensitive opplysninger som NVE besitter som kan være attraktiv for potensielle trusselaktører. Informant F nevner også en potensiell risiko for trusselaktører som kan utnytte NVEs posisjon og dermed tilegne seg bedriftssensitive opplysninger. Informant G påpeker at det kan finnes svakheter som en ekstern trusselaktør kan utnytte.

Ifølge informant E er det en grunntanke i NVE om IT-sikkerhet; «*dette skal IT-drift ta seg av, det er IT-drift som skal ta seg av IT*». Sårbarheten til NVE er denne egendefinerte beslutning om hva som er sikkert nok. Det foreligger krav om kraftsensitiv informasjon, men dette er NVEs krav til kraftvirksomheter. Informant E sa «*folk er redde for å få ansvar*» og dermed fraskriver seg ansvar om å eie et dokument heller enn å ta eierskap til det og bestemme hvem som skal få tilgang. Informant E stilte spørsmålet «*hvem eier mail*?», for å illustrere hvor vanskelig det er å fordele ansvaret.

Cybersikkerheten er, ifølge informant F, en desentralisert styrt prosess innad i NVE og er veldig ulikt håndtert avhengig av hvilken sektor man jobber i. Informant F kaller dette for en *silokultur*, som betyr at man ikke har en sømløs og tverrfaglig informasjonsflyt mellom sektorer. Ifølge informant F er det kanskje den største sårbarhet som NVE har, hvor det mangler en overordnet standard som setter krav til hvordan man skal jobbe med cybersikkerhet på tvers i NVE.

NVE foretar verdivurderinger for å kategorisere forskjellige tjenester opp mot konfidensialitet, integritet og tilgjengelighet. Denne informasjonen brukes til å vurdere hvilke verdier som har behov for skjermeverdig behandling. Ifølge informant F er denne vurderingen et «*sovende dokument som ikke er oppdatert i enkelte fagmiljøer*» noe som kan by på utfordringer når skytjenesten skal tas i bruk. Videre forteller informanten at det foregår delinger av dokumenter på kryss og tvers av sektorer. Når sektorer har egne metoder for å vurdere skjermeverdig informasjon kan det oppstå avvik i form av sensitiv informasjonsdeling med uautoriserte brukere. Informant H forteller også at det ligger forbedringselementer på å gjennomføre risikoanalyser på alle områdene. Det er en oppfatning om at å gjennomføre en ROS-analyse er en krevende jobb som kommer til å ta mye tid forteller informant H. Vurdering av sannsynlighet er en utfordrende oppgave når det gjelder cyberhendelser, vurderingsgrunnlaget er i stor grad basert på skjønn og egne vurderinger sier informant H.

En viktig del av kartleggingen er å holde oversikten over leverandørene som til enhver tid leverer tjenester til og for NVE. Leverandører og samarbeidsaktører påvirker kvaliteten på tjenestene som NVE har ansvaret for. En av de tjenestene er Splunk som nevnt tidligere. Dette endrer dagens verdikjede og informant B sier at dette endrer hvordan data blir indeksert. Videre sier inforamt B at data blir lagret på en annen plass enn det de er vant med i dag. Behandlingen av dataen skjer på en helt annen måte og krever derfor en opplæring fra leverandøren på hvordan NVE på en forsvarlig måte kan bruke plattformen Splunk. Informant D forteller at den største risikoen knyttet til leverandører er at man ikke har kontroll på leverandørene. Dette kan videre føre til brudd på integritet og konfidensialitet i form av at man deler skjermingsverdig informasjon med leverandører som i utgangspunktet ikke skulle ha tilgang på slik informasjon. Informant C forteller at man ikke kan kvalitetssikre leverandørene, men heller ansvarliggjøre dem. NVE må dermed være klar over risikoen ved å benytte seg av leverandørene der interne krav ikke kan tilfredsstilles av leverandør. Skyleverandører kan gjennomføre revisjon med frekvensavhengighet av risikoen, men NVE må selv oppdage endringer i skytjenesten som kan øke sårbarheten. Ifølge informant C, kan dette arbeidet være utfordrende. En måte NVE kan sikre seg på ved bruk av skyløsninger er, ifølge informant F, ved hjelp av domeneregistrering, applikasjonstjeneste og restriksjoner i Azure som kun er tilgjengelig for utvalgte IP-adresser.

5.1.4 DEN KRITISKE MÅLEDATAEN

Måleinstrumentene er plassert ut på de ustabile fjellpartiene for å kontinuerlig overvåke bevegelser og tilstanden. Det er kritisk at informasjonen som kommer fra måleinstrumentene for det første kommer frem til overvåkingssenteret, og for det andre at man kan stole på informasjonen som blir sendt. Nye løsninger skal gi bedre mulighet til å overvåke, som tidligere nevnt er on-premis løsningen Splunk. Splunk en mer proaktiv løsning enn Time Series Insight, ifølge informant B. Time Series Insight er den applikasjonen som følger med skytjenesten Azure fra Microsoft, men denne var ikke sterk nok til å analysere store mengder data, og ga ikke mulighet til et lukket nettverk som overvåkingssentrene ønsket, ifølge informant B. Derimot sier informant B at Splunk krever en teknologiforståelse hvor man må skaffe superbrukere på Splunk. Innføringen av Splunk fører til en endret verdikjede som påvirker hvordan data skal lagres. Dette bekymrer informant E og F, hvordan skal Splunk integreres på en forsvarlig måte. Informant F hadde heller tro på at Time Series Insight fra Azure var en bedre løsning for å minimere antall systemer som blir sammensatt. Videre sier informant F at «*jo flere systemer, jo større blir angrepsflaten*».

Informant A påpeker viktigheten av integriteten til måledata, men også den fysiske trusselen som enten kan være tilsiktet eller utilsiktet. Måleinstrumenter er, ifølge informant A, i mange tilfeller plassert på ulendte og farlige steder, men i andre tilfeller er det lett å komme til utstyret. Ved spørsmål om risikoen knyttet til den fysiske ødeleggelsen av utstyr er det for informant A kun basert på tiltro til at mennesker som oppholder seg ved måleinstrumentene ikke gjør ugjerninger. Informant A opplyser at det ikke har vært et tilfelle med fysisk ødeleggelse av måleinstrumenter, og at de med det har vært heldige. Informant B trekker også fram den fysiske trusselen som reell risiko, men at det frem til nå ikke har vært en hendelse der noen med vilje har ødelagt noen måleinstrumenter. Det foreligger, ifølge informant A, ingen formelle dokumenterte risikoanalyser over cybersikkerhet til måleinstrumentene. Men som informant A sier er det et tema som ofte blir diskutert og vurdert.

De ustabile fjellpartiene har mange ulike måleinstrument for å skape redundans i overvåkingen, i tillegg gir måleinstrumentene forskjellig informasjon om bevegelsene og tilstanden. Instrumentene skal fungere selv om resten av området har strømbrudd. Under ekstremværet Dagmar i 2011 forteller informant A at måleinstrumentene hadde strøm til tross for at fiberen var nede i dalen. Dersom måleinstrumentene skulle miste forbindelse med overvåkingssenteret blir måledata lagret hos feltpcen, som ansatte kan hente ut når

forbindelsen fungerer igjen. Måleinstrumentene er også utstyr med egne strømkilder som fuelcell, solceller og dieselaggregat for å sikre at det ikke oppstår en dominoeffekt dersom en av strømkildene skulle bli utilgjengelig. «*Tilgang til strøm for måleinstrumentene våre er akillesen vår*» (informant A).
Overvåkingssenteret har også oversikt over tilstanden til måleinstrumentene, ved behov for vedlikehold får de beskjed om dette. Avhengig av været sier informant A at personell drar ut i feltet for å reparere utstyret. Dersom været ikke tillater det må man avvente å stole på de andre måleinstrumentene. Informant A sier at måleinstrumentene blir plassert ut der geologene sier det er behov, så må overvåkingssentret selv ta en avgjørelse på om det faktisk er mulig i henhold til fremkomst. I mange tilfeller blir de plassert på ulendte områder der hvor andre mennesker ikke beveger seg. Men det er også plassert måleinstrumenter langs populære turområder hvor det er jevnlig trafikk av mennesker. Måleinstrumentene er verdifulle, ikke bare fordi de er kostbare, men også fordi de er helt nødvendige for å opprettholde den kontinuerlige overvåkningen av de risikoutsatte fjellpartiene. Den fysiske sikringen til måledata kommer i form av hengelås/kodelås, ifølge informant B, er det bare å ta med seg en tang så kan man enkelt stjele utstyret. Dersom det skulle oppstå en uønsket hendelse i form av fysisk ødeleggelse av utstyr så forteller informant A «*vi har ikke noe annet valg enn å dra ut å bytte utstyret, så enkelt er det*».

Måten overvåkingssentrene sikrer seg mot kompromittert måledata, eller tap av måledata er noe forskjellig. Informant A har sagt at de er i gang med et prosjekt med å etablere en lab hvor man kan teste teknologi og utstyr. Dette skal gi dem mulighet til å øke kunnskapen på en mer praktisk måte. Laben skal gjenskape installasjonene ute slik at alt utstyr kan bli testet på overvåkingssenteret før det blir brukt ute i feltet. Dette skal hjelpe de med å teste teknologi i tilsvarende miljø uten at det tilfører sårbarhet til systemene, samtidig skal laben hjelp til å øke kunnskapsnivået om teknologien. Videre sier informant A at de alltid velger leverandører som har den beste brannmurløsningen. Informant A sier at valg av brannmur er en prosess som blir veldig detaljert gjennomgått med leverandør før de beslutter seg til noe.

Ved spørsmål om de har sett for seg et worst case scenario forteller informant A at «*worst case scenario for oss er dersom nettverksutstyret blir hacket som fører til at vi ikke får tilgang til måledata*». For å unngå at dette skjer har de fysisk lagring av data lokalt i overvåkingssenteret og backup data hos en ekstern leverandør. De gjennomfører kontinuerlig speiling av data til ekstern lokasjon, slik at backup data alltid har oppdatert informasjon. Dette

skal sikre at nedetiden blir redusert mest mulig og måledata ikke går tapt under et potensielt angrep mot målesystemene. Men informant A sier at dette aldri har blitt teste til nå, på bakgrunn av at det er en vanskelig øvelse å gjennomføre. Dersom måledata skulle bli kompromittert ville dette, ifølge informant A, bli oppdaget relativt fort fordi det alltid sitter geologer og vurderer måledata som kommer inn.

Noen av måleinstrumentene overfører ikke dataen direkte til overvåkingssentrene, men til andre leverandører som utfører databehandling og presenterer data på leverandørens web. Informant A sier at leverandørene er aldri inne i nettverket til overvåkingssenteret, men de presenterer data på en plattform hvor en logger seg inn for å hente ut dataen. Når informantene fra overvåkingssenteret blir spurt om hvordan man forsikrer seg at leverandøren oppfyller de sikkerhetskravene som NVE måtte ha svarte informant A «*avtalen til leverandørene er prisgitt, og kravene som ligger i avtalen må en bare stole på at de oppfyller*». Noe som samsvarer med svaret fra informant B.

For tilfellet med brannmur så har de ikke mulighet til å få spisskompetanse innen brannmur og er nødt til å stole på at leverandøren etterlever avtalen. Den transnasjonale leverandøren fra Italia blir det, ifølge informant B, utført tilsyn på. Informant C forteller at det i noen tilfeller kan være at leverandøren godkjenner avtalen, og forsikrer at kravene skal være oppfylt uten å være klar over hvordan de faktisk skal oppfylle kravene. Informant A forteller at dersom det skulle være en innsider fra for eksempel radarmåling så har de ikke kontroll på det, men samtidig så har de ansatte som vurderer måledata som blir presentert og kan detektere om det oppstår merkelige dataserier.

Leverandøren av tjenesten Cautus har tilgang på måleinstrumentene totalstasjon, GPS og laser. Informant A sier at Cautus har egen VPN-konto for å logge seg på hvor overvåkingssenteret gir tilgang som blir styrt i brannmuren. I brannmuren kan de kontrollere hvilke IP-adresser som får tilgang på hvilket måleinstrument for å hindre at uautoriserte brukere får tilgang. Men her tilføyer også informant A at dersom det skulle være personer som ønsket å utføre ondsinnede handlinger så har ikke de kontroll på dette. «*Man er helt avhengige av at de på leverandørsiden er helt 100%*» (informant A).
Ved spørsmål om det er gjennomført noen ROS-analyser knyttet til digitale angrep så forteller informant A, at det ikke har blitt skriftliggjort noen analyser rettet mot digitale angrep. Fremgangsmetoden de baserer seg på er ved å gjennomgå en vurdering når ting skal bli gjort.

Frem til i dag har ikke overvåkingssenteret blitt utsatt for et målrettet angrep forteller informant A. Informant B forteller at de utfører ROS-analyser på verdien av måledata og at kontrollen på åpne porter er helt essensielt for å forsvare integriteten til måledataen. Teknologien som blir brukt både på overvåkingssentrene og ute i felt må man ha god kunnskap om, sier informant B.

5.2 DEL 2 – RESULTAT FRA RISIKOANALYSEN

I del 2 vil hovedfunn fra vedlagt risikoanalyse bli presentert, i tillegg vil en nærmere gjennomgang av hendelser som ble identifisert med høy risiko med tilhørende anbefalte sikringstiltak. Avslutningsvis vil det bli presentert generelle tekniske og organisatoriske anbefalinger som kan benyttes når man skal prioritere sikringstiltakene.

5.2.1 HOVEDFUNN FRA RISIKOANALYSEN

Risikoanalysen tok for seg totalt 60 uønskede hendelser fordelt på de tre digitale og skybaserte måleverdikjedene; intern, norsk leverandør og transnasjonal leverandør. Risikoanalysen i sin helhet ligger under vedlegg 9.5. Analysen tar for seg fire ulike hendelser i samtlige ledd av måleverdikjeden; mistet tilgang, ustabil tilgang, tap av data og kompromittert data.

Informasjon fra dokumentanalysen og intervjuene utgjør bakgrunn for antakelsene som blir fattet for sannsynlighet og konsekvens. For å vise hvordan man kommer fram til sannsynlighet og konsekvens presenteres en av antakelsene, resterende ligger vedlagt. For hendelse nr.2 ustabil tilgang, ledd: sensor, i den interne måleverdikjeden kommer følgende antakelse. Fra dokumentanalysen: Dok.nr. 2.6 sier at 7% av virksomheter ble utsatt for tjenestenektangrep i året 2017. Videre sier rapporten at 4 av 10 virksomheter blir utsatt for tjenestenekt i løpet av en måned. Fra intervju: Informant D sier at geologiske og tekniske personell har mulighet til kvalitetssikre måledata dersom de skulle vært kompromittert. Hendelsen vurderes som svært sannsynlig, karakter = 5. Hendelsens konsekvens vurderes som ufarlig, karakter = 1. En oversikt på forklaring av karakterene for konsekvens og sannsynlighet ligger vedlagt med risikoanalysen. Risikoakseptkriteriene tar utgangspunkt i tilsendte dokumenter fra NVE som heter «*prosedyre for systematisk risikovurdering*». Akseptkriteriene som NVE satt baserte seg i stor grad på skjønn kom det fram fra empiri. Noe som svekker overførbarheten betydelig da denne «skjønnsvurderingen» er subjektiv og ikke generaliserbar. Risikoakseptkriteriene er illustrert i risikomatrisen vedlagt med risikoanalysen.

Risikomatrisen vedlagt viser risikobildet for verdikjedene før og etter implementering av sikringstiltak.

Totalt ble 16 av 60 uønskede hendelser vurdert til å ha høy risiko, det vil si de hadde en sammenlagt risikoindeks (RPN) på 15 eller over. De uønskede hendelsene havnet på det røde området av risikomatrisen, og kan sies å være uakseptabel risiko. Hensikten med å gjennomføre risikovurderingen er for å kunne utarbeide råd til beslutningsgrunnlag for prioritering av sikringstiltak. Dette er grunnen for å benytte hele skalaen for risikomatrisen vedlagt. Bakgrunnen for den høye risikoen lå enten i at det var svært sannsynlig at hendelsen kom til å inntreffe, og/eller at konsekvensen for hendelsen var vurdert til såpass alvorlige for tredjepart eller organisasjonen. Ved hendelser som vurderes til å ha høy risiko skal man vurdere hvilke sikringstiltak man kan benytte seg av for å håndtere risikoen. Eksempelvis er hendelse nr.15 tap av data, ledd regionalt kontor NVE, i den interne måleverdikjeden vurdert til en risikoindeks på 16. Risikoen anses derfor som uakseptabel, håndtering av risikoen må redusere enten konsekvensene eller sannsynligheten ved å implementere sikringstiltak.

Halvparten av de uønskede hendelsene ble vurdert til middels høy risiko, det vil si de havnet på det gule området. Disse hendelsene har en risikoindeks fra og med 5 (hvor konsekvens er katastrofal, men svært lite sannsynlig) til 12 på skalaen over risikoakseptkriterier. For hendelsene i denne kategorien anbefales det at en bør foreta en videre vurdering om sikringstiltak kan påvirke risikoen positivt innenfor en forsvarlig økonomisk ramme.

De resterende 14 hendelsene ble vurdert til en akseptabel risiko, det vil si at disse havnet på det grønne området. Men dersom sikringstiltaket kan redusere risikoen bør dette vurderes etter kost-nytte prinsippet. En tydeligere framstilling av risikobildet ligger vedlagt sammen med risikoanalysen.

Fellestrekk for de uakseptable risikoene:
Etter å ha evaluert risikoanalysen kan man observere noen fellestrekk som går igjen for de uakseptable risikoene. Utfordringene fordrer bedre håndtering av cybersikkerhet for måleverdikjeden til skredvarsling.

Avhengighet til leverandør

Den digitale og skybaserte måleverdikjeden kommer til å bli så kompleks og uoversiktlig at deteksjon av rotårsaken til en feil kan bli problematisk. Dersom man ikke klarer å avdekke feilen på et tidlig stadium kan man risikere at den forplanter seg videre inn i systemene. Dette kan medføre at tjenesten som leverandøren leverer blir utilgjengelig og lammer den digitale og skybaserte måleverdikjeden til skredvarsling. Dette skjer som følge av at NVE ikke har kartlagt egne sårbarheter relatert til leverandøravhengigheten.

For skyløsningen blir NVE nærmest tvunget til å kjøre systemet slik Microsoft har designet det. Dette utgjør en betydelig risiko for å vurdere og etablere gode sikringstiltak, fordi dette er noe som Microsoft ikke tilbyr i sine applikasjoner. Som informant C sa så oppstår det en «take it, or leave it» situasjon fordi Microsoft, uavhengig av NVE, har et etablert system som de ikke vil spesialtilpasse for å tilfredsstille NVE sine krav. Videre må NVE ha mulighet til å kunne flytte løsningen fra en skyleverandør til en annen, slik at en ikke skaper synkroniseringseffekter, eller såkalte «lock-in effekter» hvor det skaper stor avhengighet hos en leverandør og høye omkostninger ved å bytte.

Utilstrekkelig kontroll av leverandør og underleverandør

Den digitale og skybaserte måleverdikjeden er avhengige av sine leverandører og underleverandører for å opprettholde kapabiliteten til skredvarslingen. Mye av sikkerheten knyttet til dagens kontroll av leverandører og underleverandører er basert på tillit. En tillit som går ut på at leverandører overholder sine løfter i leverandøravtalen. Det er lite som tyder på at det blir gjennomført rutinemessige kontroller av alle leverandørene. For NVE vil det være vanskelig å kontrollere åpne porter i nettverket, eller i brannmurer som leverandørene benytter. Har man ikke kontroll på åpne porter vil man også kunne være sårbare for potensielle utnyttelser av åpne portene. Dette kan føre til brudd på integritet, konfidensialitet og tilgjengelighet. Integriteten blir påvirker fordi uautoriserte brukere kan få tak i måledata og endre på informasjon slik at integriteten blir svekket. På samme måte kan konfidensiell informasjon slik som skjermeverdig informasjon om kraftbransjen bli lekket til uautoriserte brukere. For tilgjengelighet vil det kunne påvirke kapabiliteten til varslingstjenesten varsom.no dersom tap av måledata svekker beslutningsgrunnlaget for å vurdere ustabile fjellparti.

Mangelfulle risikoanalyser

NVE er nødt til å ha et styringssystem som tar for seg risikoanalysen sett i perspektiv av måleverdikjeden. Risikovurderingen skal kartlegge avhengighetene til leverandørene, samt sikringstiltak for å opprettholde kapabiliteten til måleverdikjeden. Mangelfulle risikovurderinger kan potensielt føre til dårligere beslutningsgrunnlag for gode sikringstiltak. Det kan også medføre at sårbarheter ikke blir identifisert og håndtert deretter. Et eksempel på sårbarhet kan være risikoen knyttet til sikkerhetskopi i skyløsningen. Azure har en innebygd redundant løsning hvor man kan få mulighet til å hente opp data som er opptil 90 dager gamle, NVE må derfor vurderer konsekvenser for potensielt evig tap av data.

Mangelfulle rammeverk for informasjonssikkerhet

NVE må ha et sentralisert rammeverk for å håndtere informasjonssikkerhet. Mangelfulle rammeverk gjør det vanskeligere for NVE å avgjøre hva det forsvarlige sikkerhetsnivået er. Det blir også vanskelig å gjennomføre gode nok risikovurderinger som gir noen retningslinjer på hva som er akseptabel risiko. Mange av hendelsene i risikoanalysen peker på svakheter for brukerrettigheter og ansvarsroller. Risikoen oppstår når man skal dele dokumenter, og kategorisere dokumenter som skjermingsverdig informasjon.

I skyløsningen Azure har ansatte selv mulighet til å tildele tilgang til dokumenter og mapper. Ansatte kan komme til skade for å dele dokumenter, samt brukerrettigheter som i utgangspunktet ikke burde vært delt. Selv om NVE deler mye informasjon offentlig, har NVE også mye kraftsensitive opplysninger om andre virksomheter. Uautoriserte brukere kan dermed få tilgangsstyring i dokumenter som kan påvirke integriteten til informasjonen.

Manglende brukeropplæring

Fra risikoanalysen kommer det frem flere ganger svikt som følge av manglende kompetanse. Dårlige passord, eller uforsvarlig oppbevaring av passord er fremdeles en risikofaktor som er høyst sannsynlig. Dersom ansattes kredentialer kommer på avveie vil det få store konsekvenser for integritet, tilgjengelighet og konfidensialitet. Konsekvensene kommer til å bli enda større ved overgangen til skyløsning fordi trusselaktøren får mulighet til å tildele egne brukerrettigheter. Videre kan trusselaktøren, til tross for at den ansatte skifter passord, ha mulighet til å utnytte tilgangene som vedkommende la inn.

I en overgang fra dagens lokale løsning til en skyløsning må ansatte ha tilstrekkelig med kunnskap og kompetanse om hvordan løsningen fungerer. Ikke bare for NVE sitt regionale kontor, men også for overvåkingssentrene hvor overgangen til Splunk fordrer tilstrekkelig med kunnskap og kompetanse. For skyløsningen innebærer dette at data ikke lengre lagres hos NVE, men i en serverpark som leverandøren drifter. Å lagre all data i en serverpark, uten en overordnet prosedyre på for eksempel kategorisering av skjermingsverdig informasjon vil være en utfordring. Dette kan føre til brudd på konfidensialitet, og integritet dersom manglende brukeropplæring om tilgangsstyring, brukerrettigheter ol. uteblir.

Innsideren

Innsideren med onde intensjoner om å skade NVE sitt omdømme eller som blir utnyttet av utenlandske aktører. Uansett hvilken type innsider det er snakk om må man kunne forvente at det kan skje, og følgende utvikle sikringstiltak. NVE må ha oversikt over alle brukere som har tilgang til systemene som inngår i måleverdikjeden, det må etableres gode rutiner som sørger for en kontinuerlig oppdatering av tildelinger, spesielt midlertidige tilganger og tidligere ansatte. Videre må de begrense lekkasje av brukerrettigheter ved å tildele færrest mulig rettigheter for brukere og begrense brukere med administrasjonsrettigheter. Det må også ligge kompetansehevende midler for å styrke den menneskelige faktoren for å unngå menneskelige feil.

5.2.2 PRESENTASJON AV HENDELSER KLASSIFISERT SOM HØYRISIKOELEMENT

Intern verdikjede

Nr.	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalte tiltak
					S	K	RPN	
3	Tap av data	-Åpne porter i nettverket -Strømbrudd -Fysisk ødeleggelse av måleinstrument -Manglende risikovurdering	Overvåkingssenteret får ikke kritiske måledata som gir utslag på vurderingsgrunnlaget til videre analyse av ustabile fjellparti.	-Overvåking tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	3	5	15	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument
11	Tap av data	-Åpne porter i brannmur -Manglende risikovurderinger - Innsider -Manglende sikkerhetskopi -Manglende forståelse av Splunk -Menneskelige feilhandlinger -Manglende autentisering av grensesnitt	Nåtidens analyse, men også fremtidige analyser, påvirkes som følge av tap av måledata. Dette vil få ringvirkninger til den kritiske samfunns-funksjonen skredvarsling som følge av manglende beslutnings-grunnlag.	-Oversikt over alle åpne porter i brannmuren (security by default) -Restriksjoner av brukerrettigheter -Ekstern lagring av sikkerhetskopi	3	5	15	-Beredskapsplan -Bevisstgjøring av ansatte -Logganalyse
15	Tap av data	-Mangelfulle risikovurderinger -Manglede sikkerhetskopi som følge av skyløsningens lagringsprosedyre -Innsider -Manglende selskapsgjennomgang av skyleverandør -Manglende oversikt over grensesnitt -Åpne kildekode program (frigir kode for en type lisens)	Avhengighet til skyleverandør fører til at NVE ikke har kompetanse til å ha løpende vurdering hvorvidt data er trygt oppbevart eller ikke. Leverandør har også mulighet til å påkoste økonomiske påkjenninger for at NVE skal være sikre på at data blir forsvarlig oppbevart.	-Risikovurdering av skyleverandør -Risikovurdering for lagring av data hos skyleverandør -Ekstern strømkilde -Sikkerhetskopi -Brannmur	4	4	16	-Løpende vurdering av skyleverandør -Vurdere å benytte flere ulike tjenester fra ulike skyleverandør for å minimere avhengighet til en leverandør, men må holde oversikt
19	Tap av data	-Lekkasje av brukerrettigheter -Innsider fjerner tilsiktet eller utilsiktet data	Data som gir grunnlaget til informasjon som publiseres er borte, slik at det fører til brudd på	-Restriksjoner til brukerrettigheter -Sikkerhetskopi	3	5	15	-Logganalyse av brukere - Kryptert ekstern sikkerhetskopi

		-Manglende etterlevelse av lover og regler	den kritiske samfunnsfunksjonen varslingstjenesten.	-Oversikt over åpne porter i brannmur (security by default)				-Logging av brannmur og tjenester

Norsk leverandør verdikjede

Nr.	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
3	Tap av data	-Manglende fysisk sikring av måleinstrument -Åpne porter i nettverket -Strømbrudd -Manglende risikovurdering	Overvåkingssenteret får ikke kritiske måledata som gir utslag på vurderingsgrunnlaget til videre analyse av ustabile fjellparti.	-Overvåking tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	3	5	15	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument
7	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data -Ukryptert trådløs aksesspunkt -Åpne porter i nettverket -Manglende sikkerhetsoppdatering -Manglende risikovurdering -Åpne porter i brannmuren	Mister kritiske måledata til å vurdere tilstand til risikoutsatte fjellparti.	-Restriksjoner til brukerrettigheter -Sikkerhetskopi -IDS -Oversikt over åpne porter i brannmur (security by default)	3	5	15	-Logganalyse -Ekstern sikkerhetskopi hos leverandør -Opplæring
8	Data er kom-promittert	-Åpne porter i brannmuren -Ukryptert kommunikasjon fra måleinstrument til dataserver -Innsider lekker informasjon -Dårlige passord	Ekstern leverandør får tilgang til sensitiv informasjon og kan ta seg videre inn i nettverket. Skjermingsverdig informasjon blir distribuert/endret slik at informasjon mister sin integritet.	-Inngått avtale med leverandør som skal overholde krav -Lukket nettverk for å hindre lateral spredning -VPN-konto	4	4	16	-Løpende kontroll av leverandør -Tydeliggjøre sikkerhetskrav -Logganalyse
9	Mister tilgang	-Nettverksbrudd -Phishing fører til at autorisert bruker ikke får tilgang -Medbragte ikke-forvaltede enheter -Dårlige passord -Manglende kartlegging av avhengighet til leverandør	Ikke-forvaltede enheter kan være infisert av trojaner eller virus som ønsker å spre seg til andre enheter, stor spredning inn i nettet kan føre til et botnet tjenestenektangrep.	-Ekstern strømkilde -E-post filtrering -Segregert nettverk -Opplæring	4	4	16	-Beredskapsplan -Bevisstgjøring for behandling av e-post -Restriksjoner for medbragte ikke-forvaltede enheter -Maskingeneret passord
15	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data uten sikkerhetskopi	Kritisk måledata eller annen skjermeverdig informasjon	-Ekstern strømkilde -Sikkerhetskopi	4	4	16	-Prosedyre for å fjerne rettigheter for brukere

		-Menneskelige feilhandlinger fører til tap av data -Mangelfulle risikovurderinger -Manglende etterlevelse av lover, regler og interne krav -Tailgating -Manglende grensesnitt i dataisolasjon	som er nødvendig for å kunne anslå beredskapsnivået til risikoutsatte fjellparti borte, slik at det vil kunne påvirke fremtidige og nåtidens situasjon.	-Restriksjon til brukerrettighet for fjerning av data -Ansvarliggjøring av leverandør -To-faktors autentifisering				-Opplæring og bevissthet om håndtering av data -Ekstern lagring av sikkerhetskopi -Grundig løpende vurdering av leverandører
19	Tap av data	-Manglende risikovurdering -Manglende sikkerhetsoppdatering -Innsider utfører tilsiktet eller utilsiktet fjerning av data -Organisatoriske endringer hos skyløsningen Azure	Data som gir grunnlaget til informasjon som publiseres er borte, slik at det fører til brudd på den kritiske samfunnsfunksjonen varslingstjenesten.	-Restriksjoner til brukerrettigheter -Sikkerhetskopi -Oversikt over åpne porter i brannmur (security by default)	3	5	15	-Logganalyse av brukere - Kryptert ekstern sikkerhetskopi -Logging av brannmur og tjenester

Transnasjonal verdikjede

Nr	**Risiko-element**	**Årsak**	**Konsekvens**	**Eksisterende sikringstiltak**	**Risikonivå**			**Anbefalt tiltak**
					S	**K**	**RPN**	
3	Tap av data	-Åpne porter i nettverket -Strømbrudd -Fysisk ødeleggelse av måleinstrument	Overvåknings-senteret får ikke kritiske måledata som gir negative konsekvens for beslutningsgrunnlaget til videre analyse av ustabile fjellparti	-Overvåking tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	**3**	**5**	**15**	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument
7	Tap av data	-Dårlige passord eller dårlig oppbevaring av passord -Manglende rutine for lagring av ulike data -Utilfredsstillende sikring av data	Mister kritiske måledata til å vurdere tilstand til risikoutsatte fjellparti.	-VPN-konto -Andre måleinstrument kan fortsatt gi data -Inngått avtale med leverandør som skal overholde krav	**3**	**5**	**15**	-Bevissthet rundt oppbevaring og vanskelighetsgrad til passord -Sikkerhetskopi -Krav til oppbevaring av data -Løpende vurdering av leverandør
8	Data er kom-promittert	- Manglende etterlevelse av lover, regler og interne krav	Måledata mister sin integritet og skjermingsverdig infrastruktur kan bli påvirket som følge av misvisende måledata.	-Inngått avtale med leverandør som skal overholde krav -Lukket nettverk for å hindre lateral spredning	**4**	**4**	**16**	-Løpende kontroll av leverandør -Tydeliggjøre sikkerhetskrav -Logganalyse
11	Tap av data	-Mangelfull tilgangsstyring -Manglende segregering av nettverk	Historiske data og sanntidsdata som er nødvendig for videre analyse svekker beslutningsgrunnlag for	-Brannmur -Oversikt over brukerrettigheter -Opplæring	**4**	**5**	**20**	-Beredskaps-plan -Fysisk sikring av stedet til server -Ekstern lagring av data

		-Manglende sikkerhetsoppdatering -Manglende opplæring -Manglede sikkerhetskopi som følge av skyløsningens lagringsprosedyre -Datainnbrudd	beredskapsnivået tilknyttet risikoutsatte fjellparti.	-Inngått avtale med ekstern leverandør				-Kvalitetssikre skyleverandørs rutine for oppbevaring av data
15	Tap av data	-Strømbrudd som følge av målrettet angrep mot strømkilde -Innsider fjerner tilsiktet eller utilsiktet data uten sikkerhetskopi -Manglende etterlevelse av lover, regler og interne krav -Tailgating	Kritisk måledata eller annen skjermeverdig informasjon som er nødvendig for å kunne anslå beredskapsnivået til risikoutsatte fjellparti borte, slik at det vil kunne påvirke fremtidige og nåtidens situasjon.	-Ekstern strømkilde -Sikkerhetskopi -Restriksjon til brukerrettighet for fjerning av data -Ansvarliggjøring av leverandør -To-faktors autentifisering	**4**	**5**	**20**	-Beredskapsplan -Ekstern sikkerhetskopi -Krav til oppbevaring av data -Løpende kvalitetssikring av leverandør
19	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data uten sikkerhetskopi -Åpne porter i brannmuren som lar uautorisert IP-adresse tilgang til systemet -Manglende brukeropplæring	Data som gir grunnlaget til informasjon som publiseres er borte, slik at det fører til brudd på den kritiske samfunnsfunksjonen varslingstjenesten.	-Restriksjoner til brukerrettigheter -Sikkerhetskopi -Oversikt over åpne porter i brannmur (security by default)	**3**	**5**	**15**	-Logganalyse av brukere - Kryptert ekstern sikkerhetskopi -Logging av brannmur og tjenester

5.2.3 ANBEFALTE SIKRINGSTILTAK

Når man skal vurdere sikringstiltak for en verdikjede er det viktig å se på tiltak som kan implementeres tidlig i de første leddene for å stoppe en videre eskalering. Helt sentralt for verdikjeder er Reasons sveitersostmodell som viser til svakheter sikringstiltakene eventuelt kan ha, og som sammenfallende kan føre til en uønsket hendelse. Eksisterende sikringstiltak og nye sikringstiltak må derfor vurderes sammen for å skape redundans. Fra risikoanalysen kommer det frem at flest uønskede hendelser er knyttet til de eksterne verdikjedene. Derfor bør sikringstiltak prioriteres for de eksterne verdikjedene for å minimere antall sårbarheter. Hentet ut fra risikoanalysen vedlagt for å illustrere dette: For hendelsen nr.8 kompromittert data i måleverdikjeden for norsk leverandør, ledd: NORSAR/NORCE kommer følgende forklaring til ny risikoindeks. Løpende kontroll av leverandører vil kunne redusere sannsynligheten for at data blir kompromittert. Tydeliggjøring av sikkerhetskrav, restriksjoner for brukerrettigheter sammen med logganalyse vil bidra til å redusere konsekvensene for data som blir kompromittert. Den nye risikoindeksen vil dermed bli vurdert til sannsynlig (karakter = 3) og konsekvensen redusert fra kritisk til farlig (karakter = 3). Vedlagt ligger alle beskrivelsene for den nye risikoindeksen, samt risikomatrisene som illustrerer risikobildet før og etter implementert sikringstiltak. Der hvor risikoen ikke lar seg bli redusert, det kan være en sannsynlighet for innsider, bør det vurderes å utarbeide en beredskapsplan som kan iverksettes dersom hendelsen skulle inntreffe.

Anbefalte organisatoriske sikringstiltak går innunder prinsippene fra Resilience Engineeringsteorien:

1. Læring – bevisstgjøre ansatte ved å investere tid og ressurser til å generere kunnskap om teknologien. Kunnskap generes ved å gjennomføre risikoanalyser, kompetansehevende kurs og testing av teknologi.
2. Respondere – rask respons, også fornuftig respons fordrer en beredskapsplan som integreres inn i styringssystemet. Kunnskap om hvordan ulike hendelser oppfører seg bør også være en del av beredskapsarbeidet, samt en kommunikasjonsplan for verdikjeden slik at nødvendig respons blir spredd til berørte ledd
3. Overvåke – logganalyse, revisjonskontroll av leverandører, oversikt over brukerrettigheter. Konkrete tiltak som sammen skal detektere sikkerhetsbrudd på et tidlig stadium for å hindre eskalering og videre spredning.

4. Forutse – kontinuerlige vurderinger og analyser før implementasjon av ny teknologi, eller ved oppdatering skal avdekke potensielle sikkerhetsbrudd.

Anbefalte tekniske sikringstiltak vil ha god effekt for å sikre den digitale og skybasert måleverdikjede for fjellskredvarsling:

- Segregerte nettverk – for å hindre uautoriserte brukere å nå inn til skjermingsverdig informasjon bør det i APIene lages datagrensesnitt i skyen. I tillegg vil det forhindre lateral spredning i nettverket.
- Brukerrestriksjoner – ikke tildel administratorrettigheter til «vanlige» brukere for å hindre lekkasje av rettigheter og kompromitterte data. Dette er spesielt viktig for skyløsning da denne fort kan lekke som følge av at feks. feil i kopifelt fører til at en uautorisert bruker får tilgang til skjermingsverdig informasjon.
- Logganalyse – for å vite hva som har skjedd og bidrar til å oppdage sikkerhetsbrudd tidlig. Hva som bør logges er eksempelvis unormalt datavolum (kan være en indikasjon på tjenestenektangrep), påloggingsforsøk, unormal aktivitet rundt tilkoblinger.
- Inntrengingstester – for å avdekke eventuelle sårbarheter i infrastrukturen langs måleverdikjeden, dette kravet bør også kommuniseres til leverandører av måleverdikjeden.
- Security by design/security by default – for å få oversikt over alle åpne porter i brannmurer, rutere og svitsjer.
- Ende-til-ende kryptering – for å sikre kommunikasjonen mellom tjener og server, samt bevare integriteten og konfidensialiteten til informasjon.
- Maskingenererte passord – for å forhindre den menneskelige feilhandlingen med å lage svake passord.
- To-faktors autentisering – for å sikre at autoriserte brukere får tilgang til systemet, og uautoriserte brukere adgangsnekt.

NVE bør også ha et overordnet rammeverk for håndtering av informasjonssikkerhet i måleverdikjeden. Rammeverket bør kommuniseres og distribueres internt og til leverandørene. Dette for å sikre forankring av sikkerhetskultur hos leverandør for den kritiske samfunnsfunksjonen skredvarsling, men også for å ansvarliggjøre og bevisstgjøre hele verdikjeden. I rammeverket skal det foreligge en overordnet prosedyrer som tar utgangspunkt

i Schifloes tilnærming for vurdering av samfunnssikkerhet for ulike aktiviteter som skal detektere og forebygge sikkerhetsbrudd på et overordnet nivå. Dette for å forhindre at risikoanalyser tar utgangspunkt i en risiko som alene er ubetydelig, men som i helheten vil utgjøre en sårbarhet. Dette kan eksempelvis være et tjenestenektangrep som fører til ustabil tilgang. Ustabil tilgang vil ikke alene være en risikofaktor, men ustabil tilgang i måleverdikjeden kan føre til at kritiske måledata ikke når fram til varslingsportalen varsom.no. Det må også foreligge en prosedyre for å kategorisere skjermingsverdig og kraftsensitiv informasjon. Følgelig skal det vise til hvordan skjermingsverdig informasjonen skal behandles i henhold til prinsippene integritet, konfidensialitet og tilgjengelighet. Videre skal rammeverket vise til ansvarsrollen ansatte har for håndtering av skjermingsverdig informasjon. Det vil si klare retningslinjer for blant annet deling av brukerrettigheter, datadelingsgrensesnitt og forsvarlige passord.

6 KAPITTEL: DRØFTING

Kapittelet skal presentere oppsummeringen av analyse og empiri, hvor empiri skal drøftes opp mot det teoretiske bidraget til studiet. Strukturen før kapittelet er delt inn i tematiske utfordringer som anses grunnleggende for å svare ut forskningsspørsmålene. Drøftingen underbygger de sårbarhetene som er relevante å vurdere for å sikre den digitale og skybaserte måleverdikjeden.

6.1 DEN DIGITALE VERDIKJEDEN – EN KJEDE ER ALDRI STERKERE ENN SITT SVAKESTE LEDD

One how knows the enemy and knows himself will not be in danger in a hundred battles.
One who does not know the enemy but knows himself will sometimes win, sometimes lose.
One who does not know the enemy and does not know himself will be in danger every battle.

– (Sun Tzu Wu)

Det kjente ordtaket fra generalen Sun Tzu Wu skildrer utfordringene i trusselbildet i det digitale rom. I overført betydning kan det tolkes slik at man bedre kan håndtere trusselaktørene ved å ha god kjennskap til hva man ønsker å beskytte og hvordan man skal identifisere egne sårbarheter og svakheter. Det å kjenne seg selv betyr i denne sammenheng å vite hvilke verdier man ønsker å beskytte, og hvordan identifisere sårbarheter og svakheter som en trusselaktør kan utnytte. Videre bør man avklare hvilke aktører som kan nyttiggjøre seg av de verdiene. Har man svarene på dette vil man i større grad være i stand til å beskytte

seg mot truslene, men kompleksiteten som følge av økt digitalisering gjør det vanskelig å komme frem til et enkelt svar. Trefaktormodellen som ble beskrevet i teorien er et slikt hjelpemiddel som kan hjelpe NVE med å kjenne fienden og seg selv. Trefaktormodellen representerer sårbarhet, trussel og verdi hvor risiko står som sentralt utgangspunkt for å detektere de tre faktorene. Dersom man benytter trefaktormodellen har man, ifølge ordtaket til Sun Tzu Wu, et godt utgangpunkt for å være i stand til å beskytte sine verdier mot hundre potensielle angrep. Trefaktormodellen kan man kartlegge ved hjelp av den tradisjonelle risikostyringsmetodikken fra ISO 31000, eller NSMs grunnprinsipper for IKT-sikkerhet. Supplert med et godt styringssystem for å kartlegge sine digitale verdikjeder, fra for eksempel DSB sin veileder om risikostyring for digitale verdikjeder. Men hvorfor er det fremdeles så mange uakseptable risikoer som ble kartlagt i risikoanalysen? Det er en mulighet at dagens rammeverk og metodikk ikke er tilpasset godt nok for en kritisk samfunnsfunksjon som skredvarsling.

NVEs digitale verdikjede blir uoversiktlig og kompleks med stadig tettere koblede systemer som er gjensidig avhengig av hverandre. Å identifisere alle sårbarheter, svakheter og avhengigheter igjennom hele verdikjeden er utfordrende. Det blir enda mer utfordrende for de verdikjedene som er underlagt annen jurisdiksjon, hvor NVE i liten grad kan kontrollere sikkerheten utover det som er regulert i den privatrettslige kontrakten. Dette gjenspeiles også i risikoanalysen for den eksterne og den transnasjonale verdikjeden. Antallet uakseptable risikoer er høyere sammenlignet med den interne verdikjeden, og det er i stor grad fordi påvirkningskraften NVE har til disse verdikjedene er mindre. NVE har derfor et behov for blant annet et overordnet rammeverk som viser hvem som skal ha ansvaret for leverandører. Uten denne kontrollen vil NVE ikke klare å kartlegge sine sårbarheter i den digitale og skybaserte måleverdikjeden. Ifølge Perrow (1984) sin teori om normalulykker vil måleverdikjeden være utsatt for normalulykker, fordi den hverken kan styres sentralisert eller desentralisert. Måleverdikjeden er sammensatt av tette koplinger og har høy grad av interaktiv kompleksitet, noe som kan gjenspeiles i den kritiske måledataen. Tap av måledata vil være katastrofalt for hele måleverdikjeden, noe som kommer frem i risikoanalysen vedlagt. For den uønskede hendelsen nr.11 tap av data (ref. Risikoanalysen, intern, ledd: Stranda) vil det være følgende konsekvens: «*Nåtidens analyse, men også fremtidige analyser, påvirkes som følge av tap av måledata. Dette vil få ringvirkninger til den kritiske samfunnsfunksjonen skredvarsling som følge av manglende beslutningsgrunnlag*.» Dette eksemplifiserer teorien om normalulykker, hvor en komponentfeil rask fører til betydelige endringer for andre

hendelser, fordi det er vanskelig å stoppe hendelsesforløpet i en tett koplet og kompleks verdikjede [48]. Risikobildet fremover vil nok i stor grad være preget av gjensidige avhengigheter for den digitale og skybaserte måleverdikjeden.
«Avhengigheter mellom samfunnsfunksjoner skaper effektivitet og bedre tjenesteleveranser, men kan også gi sårbarheter ved at feil som oppstår ett sted i en verdikjede, kan forplante seg» [55, p. 8].

NVE er et attraktivt mål grunnet sin maktposisjon med å forvalte blant annet vassdrag og energi til Norge og utlandet. Leverandørene og underleverandørene er også betydelig utsatt for potensielle målrettede angrep, på bakgrunn av tilknytningen de har til NVE. Kommunikasjon mellom NVE og kunde er som nevnt et potensielt scenario som kan utnyttes av en trusselaktør, ifølge informant F. Dette scenarioet utspilte seg i virkeligheten for virksomheten Norfund. I mai 2020 publiserte Norfund at de ble utsatt for en alvorlig svindel som følge av et avansert dataangrep. Norfund mistet 100 millioner kroner som en av konsekvensene ved dataangrepet, hvor svindlerne manipulerte informasjonsutvekslingen mellom Norfund og låntager over tid [58]. Det å misbruke NVEs maktposisjonen mot sine brukere av NVEs tjenester, leverandører og underleverandører kan være et realistisk scenario. For å oppdage en slik svindel må NVE ha kontroll over sine verdikjeder, og ansatte må være bevisste på at slike hendelser er reelle.

Hvordan skal man redusere sårbarheten i de uoversiktlige, komplekse, tett koblede og transnasjonale digitale verdikjedene? Det hele ligger på sikkerhetskulturen som må være til stede i samtlige ledd av verdikjeden, og etterleves av leverandører og underleverandører. Et styringssystem som NSMs grunnprinsipp kan være en måte å redusere denne sårbarheten på. Ved å legge til rette for at grunnprinsippene også etterleves av leverandører og underleverandører. Ansatte fra NVE må være i stand til å kontrollere at grunnprinsippene til enhver tid blir overholdt av leverandører i form av revisjon, stikkprøver eller lignende former for bekreftelser. Informantene sier de er prisgitt til avtalen som de inngår med leverandørene for at de overholder visse kriterier og krav til den tjenesten som utsettes. NVE legger derfor sin tillit til at leverandører overholder elementene i avtalen, men som informant C sier kan det oppstå situasjoner der leverandører lover noe som de ikke har mulighet til å overholde. Det kan være ulike årsaker til hvorfor dette skjer, men det kan skje, og at dette må tas med i betraktningen når NVE inngår en avtale med en leverandør. NVE må kunne vite hvordan de skal håndtere en situasjon som oppstår som følge av en feil hos leverandør for å kunne

forsvare sine verdier. Her kommer begrepet ytelsesvariasjon inn som en viktig faktor, å vite hvordan man håndtere en dynamisk situasjon som kjennetegner en cyberhendelse. Man må kunne forvente det uforventede, og i den digitale verdikjeden er det mange muligheter som kan føre til et sikkerhetsbrudd. Det viktigste organisatoriske hjelpemiddelet i en digital verdikjede er menneskets evne til å kommunisere for å hindre lateral spredning. Til tross for at informant B sier at årsaken til sikkerhetsbrudd i 20-50% av tilfellene er menneskelige feilhandlinger, er det også som informant D sier, at mennesket som er det sterkeste leddet. Mennesket har en vurderingsevne basert på skjønn som ikke lar seg standardiseres i en programvare. Eksempelet som informant D brukte skildrer menneskets ytelsesvariasjon på en god måte. «*Kompromittert måledata kan bli vurdert av fagpersonell på overvåkingssenteret til å si at disse målingene ikke samsvarer med egne observasjoner og at man deretter raskt kan gjøre nødvendige tiltak*». Denne skildringen beskriver hvordan prinsippene i teorien om Resilience Engineering fungerer i praksis – hvor mennesket utnytter den ytelsesvariasjonen til å fatte en beslutning basert på kunnskap, erfaring og intuisjon.

En risikofaktor som nevnes flere ganger både i risikoanalysen og intervjuene er innsideren. Denne innsideren kan bevisst eller ubevisst lekke informasjon. Hvordan skal man kunne ha oversikt over alle eventualiteter om en innsider i den digitale verdikjeden? Ifølge informantene er dette en umulig oppgave, da NVE hverken har nok kompetanse eller ressurser til å holde løpende kontroll over sine leverandører og ansatte. Fra risikoanalysen vedlagt vil det også knyttes stor usikkerhet til vurderingen av sannsynligheten for en innsider. Sikringstiltak som anbefales er brukerrettigheter. Man må gi færrest mulig brukerrettigheter for å minimere konsekvensene, men det vil ikke minimere sannsynligheten. Risikoen vil øke betydelig i overgangen til skyløsningen da ansatte selv tildeler rettigheter, og med uoppmerksomhet kan tildele uautoriserte brukere tilgang. Dette blir ansett som en stor risikofaktor i risikoanalysen når det gjelder integriteten og konfidensialiteten til informasjon.

Fra empirien kommer det frem at det registreres opptil flere forsøk på angrep daglig, med alt fra virus, til mistenkelig email. En skremmende utvikling som kom frem fra empirien er at forsøkene nå er så avanserte at man nesten må være utdannet cybersikkerhetsekspert for å se at dette er et forsøk på svindel. Når metodene blir så avanserte og intrikate ligger mye av utfallet på beslutninger som tas eller ikke tas av den ansatte i det avgjørende sekundet. For mange oppleves dette som en arbeidsoppgave de ikke ønsker å ha ansvar for. Mangelfull kunnskap og for lite fokus på sikkerhetskultur, fører til at ansatte gjør feil eller fraskriver seg

ansvaret og pusher det videre i organisasjonen. I teorien om sikkerhetskultur fremmer man åpenhet, og å rapportere om «nesten-hendelser» blir ansett som positivt fordi det gir lærdom. Menneskelige feilhandlinger kommer alltid til å være en del av trusselen, men for å være bevisst over mangler krever det at NVE utfører risikovurderinger kontinuerlig som ikke bare er sektorbasert. Flere av informantene peker på forbedringselementer i å gjennomføre risikovurderinger for alle sektorene. NSM trakk også fram i sin rapport at en stor andel virksomheter hadde mangelfulle risikovurderinger [55]. Mangelfulle risikovurderinger kan ikke bare føre til at sårbarheter ikke blir identifisert, men effektgraden til sikringstiltakene kan i stor grad bli påvirket som følge av mangelfull risikovurdering. Man kan risikere å implementere tiltak som ikke har noe hensikt eller effekt for å redusere risikoen. Dette kan utgjøre en trussel i form av en falsk følelse av trygghet, der hvor man lever i tro om at man har beskyttet sine verdier på en forsvarlig måte, men i realiteten så har sikringstiltaket ingen beskyttelsesfunksjon. I tillegg kan en risikovurdering være det verktøyet som vurderer effektgraden til tidligere implementerte sikringstiltak. Skulle et sikkerhetsbrudd oppstå vil en risikovurdering kunne fortelle hvilke sikringstiltak som allerede var implementert, og hvor sårbarheten til dette sikringstiltaket befinner seg. Ut ifra vurderingen vet man hvor sikringstiltaket bør implementeres, og hva som skal til for å bygge et forsvar i dybden. Risikovurderinger er også det verktøyet som bør tas i bruk for å implementere ny teknologi, slik som digitale målere og skyløsning, på en forsvarlig måte.

Metodikken risikoanalysen krever også at NVE er flink til å kontinuerlig jobbe med risikostyring. For ved å gjennomføre en risikoanalyse kan det skape en illusjon om at det er forsvarlig sikret, at systemet i sin helhet er fullstendig sikkert, noe som ikke er tilfellet. Det vil alltid være både en restrisiko som ikke lar seg reduseres ved implementert tiltak. Det vil også alltid være uforutsette hendelser som fører til en ny situasjon og oppfører seg helt uventet i forhold til det risikoanalysen tilsier. Risikoanalyse er et verktøy som må integreres i NVEs årshjul som en del av virksomhetsstyringen og ansatte må ta mer selvstendig ansvar for å rapportere inn hendelser og nesten-hendelser. Dette er spesielt viktig i cybersikkerhet da et sikkerhetsbrudd raskt kan forplantet seg et annet sted i nettverket eller at det ikke blir oppdaget i det hele tatt. Sikkerhetskultur blir med andre ord avgjørende for å sørge for en dynamisk og kontinuerlig tilnærming til de løpende risikovurderingene, hvor ansatte kan benytte risikoanalysen som et verktøy og rammeverket som retningslinjer til å ta gode beslutninger.

6.2 INTENSJON OG KONSEKVENS MED TEKNOLOGI OG SKYLØSNING

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

– Bruce Schneier

En av årsakene til den raske digitaliseringen er at teknologien skal bistå med mer ressurseffektive og kostnadseffektive løsninger for å gjøre arbeidsdagen enklere. Men implementeringen av teknologien skjer i dag raskere enn forståelsen av teknologien, noe som fører til et kunnskapsgap mellom forståelse og teknologi. NVE kan ikke tilfredsstille digitaliseringsbehovet bare ved å implementere digitale målere og skyløsning. De må også kunne forstå og utvikle egne ferdigheter for at digitaliseringen skal ha den tiltenkte funksjonen. Manglende kunnskap til implementert teknologien medfører naturligvis sårbarheter. Sikringstiltak for å redusere sårbarhetene hos teknologi som man ikke forstår vil heller ikke hjelpe, og er bakgrunnen for sitatet til Bruce Schneier. Sitatet belyser også essensen på denne studiens problemstilling, for å sikre verdikjeden må man ha god kjennskap til systemet, sårbarheten og ikke minst forstå teknologiens formål og anvendelse.

Funnene fra empirien er tett knyttet opp til menneskets forståelse av teknologi. Risikoanalysen viser også til en betydelig risiko for manglende kunnskap om digitale målere og skyløsningen. En av årsakene som knyttes til manglende teknologiforståelse som kommer fram fra risikoanalysen vedlagt er blant annet «*manglende oversikt over åpne porter*». Dette er knyttet opp mot skyløsningen, og hvor grensesnitt avgrenser hvor i skyen brukere kan gå. Dersom NVE ikke kartlegger alle områdene i skyen som skal være isolert kan man risikere at uautoriserte brukere får tilgang til sensitive informasjon. Et sikringstiltak som kommer frem fra intervjuene er utarbeidelsen av laben.

Å implementere nye digitale målere og skyløsningen i en kritisk måleinfrastruktur er risikabelt. Denne vurderingen må ha godt nok grunnlag for potensielle avveininger. Fra empirien kommer det frem flere utfordringer som blir ulikt vurdert med overgangen til skyløsningen. Den første var at skyleverandørene kun har installasjoner i utlandet. Dette er utgjør en betydelig risiko, kommer det frem fra risikoanalysen. NVE må forsikre seg at informasjonen blir forsvarlig sikret etter henhold til NVEs behov. Det var ansett som uakseptabelt for overvåkingssenteret å lagre data utenfor norsk territorium. Skyløsningen Azure hadde ved beslutningstidspunktet (vinteren 2020) ikke serverparker på norsk territorium. Overvåkingssentrene har et krav fra TEK 17 om en operativ overvåking 24/7, så

lagring av data måtte skje lokalt. Baser på dette kom forslaget om å benytte Splunk opp, som en tilleggstjeneste for at overvåkingssenter skal få samme funksjonalitet med lagre lokalt. NVE vil dermed måtte forholde seg til to systemer som skal integreres. Som nevnt tidligere fører flere systemer til større angrepsflater og potensielt mer sårbarhet. Dette er to systemer som skal snakke sammen og følgelig ha en sømløs kommunikasjon. Overvåkingssentret vil derimot fortsatt bevare sitt lukkede nett hvor informasjon går kun gå ut fra overvåkingssentret.

NSM har i sin rapport[15] nevnt at man må ha tillit til at skyleverandør oppbevarer dataen på en forsvarlig måte. De anbefaler å gjennomføre risikovurderinger dersom virksomheter vurderer å benytte seg av skyleverandører som lagrer informasjonen i utlandet. NSM har også sammenlignet med risikoanalysen vurdert at å lagre informasjon i utlandet vil utgjøre en større risiko. I tillegg påpeker NSM at vil det være mer utfordrende å holde oversikt over eierskapsstruktur og uautoriserte tilganger [55].

Menneskelige feilhandlinger er ifølge funn fra empirien en betydelig sårbarhet ikke bare ved implementering av ny teknologi, men også med nåværende teknologi. Som nevnt i empirien var det en informant som mente at den eneste løsningen på menneskelige feilhandlinger er å installere tekniske barrierer fordi mennesket uansett på et eller annet tidspunkt vil gjøre feil. Dog sier teorien om sikkerhetskultur at «*Organisasjoner kan investere tid og ressurser i å integrere teknologi som skal være mer sikret mot digitale angrep, og utarbeide systemer for adgangskontroll, men dette vil i realiteten ikke gjøre en organisasjon sikrere dersom det organisatoriske aspektet ikke gjenspeiler det teknologiske*». Teorien sier helt konkret at den teknologiske forståelsen må være til stede uavhengig av de tekniske barrierene. Kapabiliteten til de tekniske barrierene vil ikke fungere som tiltenkt dersom mennesket ikke forstår teknologien. Dette viser til Reasons sveitserostmodell som sier at de tekniske barrierene kan være utstyrt med latente forhold, som i dette tilfellet er den manglende forståelsen av teknologi, og kan sammenfallende med en menneskelig feilhandling føre til et sikkerhetsbrudd.

Ifølge informantene vil ansattes vanlige rutiner endres ved implementering av digitale målere, og ikke minst ved bruk av skyløsning. Fra empirien virker det som om informanter tenker at

[15] Risiko (2020) NSM

skyen skal være sikrere, blant annet fordi antallet brannmurer øker fra det de har i dag. Men også fordi Microsoft Azure har den kunnskapen og ressursene som trengs for å holde et forsvarlig sikkerhetsnivå. Dette underbygges i NSMs rapport som sier at skyløsninger kan bidra til bedre håndtering av cybersikkerhet fordi det skjer i store og profesjonelle miljøer [55].

Skyløsningen NVE valgte å gå for var Azure fra selskapet Microsoft. Valget baserte seg i stor grad på lettvinthet ifølge to informanter, og at man allerede hadde begynt å bruke tjenesten Office 365. Microsoft Azure åpner opp for muligheten med å kombinere historisk data sammen med sanntidsdata for å gi fremtidsrettet predikasjoner, som er en klar fordel for NVE. Microsoft blir en svært sentral leverandør og det gir en sterk avhengighet. Det er en potensiell risiko ved at NVE blir låst til et system eller en skyleverandør, hvor eventuell byttekostnad blir for høy. NSM har som nevnt i sin huskeliste sagt at man ikke må låse seg fast til en løsning og bli leverandøravhengig [55]. Dette krever en annen tilnærming enn de rammeverkene som ENISA, NSM og NIST tilbyr i dag. ENISA sitt rammeverk for sikkerhet i statlige skyer tar med elementene i forkjøpsprosessen til ferdigstilt skykontrakt, og i rammeverket viser de til den kjente metodikken om PUKK-hjulet for å opprettholde forsvarlig sikkerhetsnivå i skyløsninger. Men denne løsningen kommer som en del av et større styringssystem, som nok engang fordrer en mer helhetlig cybersikkerhetshåndtering. Rammeverkene har begrensinger som gjør det å se et helhetlig bilde mer utfordrende da det blir sentrert rundt et spesifikt system og ikke systemet som en del av en større verdikjede. I tillegg er rammeverkene reaktive i form av at en kartlegger uønskede hendelser for det som allerede har skjedd. Man får da ikke mulighet til å beskytte seg mot de ukjente truslene som kan oppstå og blir dermed mer sårbart. Ved å følge ISO-standarder kan man også kvantifisere risikoen ved å ta utgangspunkt i at risikoen er objektiv for å måle sannsynlighet og konsekvens. Når sikringstiltak er implementert og akseptrisikoen er tilfredsstilt har man da kontroll? Hvordan skal man klare å benytte denne tilnærmingen for skyløsning på en forsvarlig måte? Svaret på om man har kontroll er helt enkelt, nei det har man ikke, og man burde heller ikke ha den innstillingen om at risikostyringen er en ferdigstilt prosess. Det finnes ikke et enkelt svar på hvordan man skal benytte en slik tilnærming for skyløsning, for det vil i stor grad være avhengig av menneskets kapabilitet og ytelsesvariasjon. Det krever en god teknologisk forståelse i en større sammenheng. En forståelse om hvordan en liten komponentfeil eller brukerfeil kan medføre alvorlige konsekvenser lengre ut i en kompleks og uoversiktlig verdikjede. Anbefalingene fra Perrow, sammen med sikringstiltakene fra

risikoanalysen kan i stor grad benyttes for å beskrive de prosessene som NVE har som utfordringer.

NVE må ifølge Perrow [48]:

(1) Redusere interaktiv kompleksitet, ved å holde måleverdikjeden så lokal som mulig.
(2) Løsne tette koblinger, dette gjør de ved å ikke binde seg for mye til en leverandør som Microsoft.
(3) Desentralisert styring hos leverandørene i måleverdikjeden, fordi leverandørene har best kunnskap om risikoen knyttet til sin arbeidsoppgave.
(4) Sentralisert styring for NVE som kontrollerer at leverandørene overholder den desentraliserte styringen. NVE kan benytte metodikken fra Schiefloe (2011) for å vurdere samfunnssikkerhet, for å oppnå sentralisert styring.

Man trenger en ny måte å gjennomføre risikovurderinger på når skyløsningen blir en del av hverdagen. Rammeverkene vil ikke være tilstrekkelige nok for å oppbevare et forsvarlig sikkerhetsnivå i den kritiske måleinfrastrukturen, fordi de kun viser et bruddstykke av et større system som er veldig dynamisk og krever en mer proaktiv tilnærming. Dette krever også at andre virksomheter som har vært utsatt for tidligere hendelser er åpne om å dele sine erfaringer og kunnskap til å utvikle gode sikringstiltak som fungerer.

6.3 Tilnærming til analysemetodikk

Det må gjøres en vurdering av ulike kriterier før man gjennomfører og velger hvilken risikoanalyse man skal benytte. Typiske kriterier for en kritisk infrastruktur som måleinfrastrukturen er omfanget av metodikken, målsetting for metodikken, anvendte teknikker og standarder, innbyrdes avhengighetsdekning, om resiliens er kartlagt og om den kritiske infrastrukturen er tverrsektoriell. Bakgrunnen for at flere rammeverk er introdusert i teorien. Ved å trekke ut elementer fra de introduserte rammeverkene er håpet å kunne gi en mer dynamisk tilnærming for risikoanalysemetodikk som gir svar som også kan ses i et samfunnsperspektiv [35].

Studiets resultat vil være avhengig av hvilken tilnærming til risikoanalysemetode en velger å bruke, derfor var det viktig å se på hvilke svar en ønsker å få ut av analysen. Risikostyring sammen med rammeverk for informasjonssikkerhet kan bidra til den helhetlige forståelsen av sårbarheter for NVE. Ved å kombinere de rammeverkene er målet å skape en synergi for cybersikkerheten til NVE. For å oppnå synergien er det nødvendig å se rammeverkene i et

holistisk perspektiv for hele verdikjeden. Med en holistisk tilnærming kan en kartlegge flere sikkerhetshull som en potensielt kan gå glipp av i en silobasert tilnærming. I tillegg har en mulighet til å forsterke tiltak som strekker seg over flere sektorer [35].

Risikoanalysen blir styrt av den som utfører analysen, subjektiv vurdering blir avgjørende for hendelser som mangler statistikk. Den intuitive følelsen er fremtredenen faktoren i beslutningsavgjørelser knyttet til risikovurderinger [31].

6.3.1 PRESENTASJON AV ANALYSEMETODENE

Når man velger en metode fremfor en annen, må man alltid være klar over at det kan lede til ulike resultater. Kriteriene for risikoanalysen er sentrale for å kunne velge den best tilpassede metoden som kan gi de svarene en søker. Det finnes fordeler og begrensinger med alle analysene som ble presentert i teorien, men det gjelder å finne den analysemetoden hvor fordelene overveier begrensingene. I tabell 6.3.1 blir egne betraktninger til analysemetodene sammenstilt.

Rammeverk	Fordeler	Begrensinger
ISO 3100/ISO 27001	• Er i hovedsak enkel å gjennomføre • Metoden krever ingen sterk teoretisk/analytisk bakgrunn for de som utfører analysen • Gir forslag til risikoreduserende tiltak • Gir et godt grunnlag for beredskapsplanlegging • Kan bidra til å identifisere årsaken til sikkerhetsbrudd og hindre at tilsvarende skjer i fremtiden	• Er statisk i forhold til tid og sted • Bruk av ulike konsekvensdimensjoner kan innebære vanskelige avgjørelser, feks. verdisetting av menneskeliv • For tilsiktede hendelser er det generelt vanskelig å bedømme sannsynligheter • De tiltakene som kommer ut av analysen kan noen ganger stå i strid med hverandre
NIST-Cyber-security framework	• Rammeverkets språk er tilpasset både private og statlige aktører • Foreslår kostnadseffektive løsninger • Bruker kjente referanser for tverrsektorielle sektorer som er typisk for kritisk infrastruktur	• Omfattende analyse som er ressurskrevende • Må ha kjennskap til alle lover og retningslinjer for analyseobjektet • Vanskelig å si noe om en reell effekt av et risikoreduserende tiltak
ENISA – Cloud Computing	• Får kartlagt risikoen som er tilknyttet til implementering av skytjeneste	• Har ingen måte å vurdere kritikalitet på, dette må dermed virksomheten vurdere selv

Security Risk Assessment	• Viser hvordan vurdere hvilken skytjeneste som kan tilpasses virksomhetens behov • Har detaljerte scenarioer som fremstiller hvordan rammeverket kan bli brukt	• Generisk oversikt over de mest typiske utfordringene for virksomheter, de med ekstraordinære verdier må finne ut av dette selv
NSM – Grunn-prinsipper i IKT-sikkerhet	• Forklarer hvilke forutsetninger for at cybersikkerheten kan kunne gjennomføres i henhold til rammeverket • Enkelt å bruke som «oppskrift» til generell styringsstruktur • Kan identifisere potensielle sikkerhetsbrudd og bistå til å utarbeide en prosedyre for å håndtere hendelsen	• Generisk med oppfordring til å gjennomføre aktiviteten i henhold til et «forsvarlig sikkerhetsnivå» • Virksomheten må selv finne ut hvordan utarbeide detaljerte planer for håndtering av cyberhendelser som kan implementeres i virksomhetens egenberedskap

Tabell 6.3.1 Fordeler og begrensninger for rammeverk for cybersikkerhet

6.3.2 PRESENTASJON AV VALGT ANALYSEMETODIKK

Basert på vurderingen av de ulike tilnærmingene er det i dette studiet valgt å gå for en mer tradisjonelt rettet analysemetodikk. Den utvalgte risikoanalysen baserer seg på ISO 31000 metodikken og kan kjennetegnes for en grovanalyse. Bakgrunnen for valget er den tverrsektorielle risikoen som påvirker den kritiske samfunnsfunksjonen skredvarsling. På bakgrunn av analyseobjektet, som er et tenk scenario, er det valgt å benytte en grovanalysemetodikk med noen modifikasjoner. Grovanalysen identifiserer uønskede hendelser, deretter evalueres risikoen og til slutt kommer det forslag til risikoreduserende tiltak. En grovanalyse er et godt verktøy tidlig i konseptfasen for å få oversikt over uønskede hendelser, samt finne sårbarheter til analyseobjektet. Grovanalysen er også et godt utgangspunkt for videre arbeid med beredskapsplanlegging som er nødvendig innenfor cybersikkerhet. Grovanalysen vedlagt har også evnen til å gi en holistisk risikovurdering over verdikjeden. Dette krever dog at man har en komplett oversikt over systemet som skal analyseres og tilgang til informanter med ekspertkunnskap. Ekspertkunnskap vil være den faktoren som bedømmer sannsynlighet og konsekvens da det ikke eksisterer nok mengdedata til å ta en kvantitativ vurdering av tilsiktede hendelser innen cybersikkerhet [35].

6.4 HVEM HAR ANSVARET FOR DATAEN; ANSATTE, LEDERE ELLER LEVERANDØRER?

Each problem that I solved became a rule which served afterwards to solve other problems
– René Descartes

Som siste delen av risikostyringsprosessen skal man følge opp og kommunisere risiko. Risikokommunikasjon er en helt sentral del av risikostyringsprosessen, i hvert fall når man er en del av den digital måleverdikjede for skredvarsling. Hvem skal ha ansvaret for å videreformidle risikoen i måleverdikjeden, når risikokommunikasjonen for måleverdikjeden innenfor NVE blir styrt desentralisert? Når informantene peker på en desentralisert håndtering av cybersikkerhet vil det naturligvis være fordeler med det, men det vil også være noen betydelige ulemper. Fordeler med en desentralisert håndtering er at hvert fagområde som håndterer risiko har kjennskapen til sin egen arbeidsoppgave, og vet hva som kan føre til sikkerhetsbrudd. De har derfor mulighet til å, ut ifra erfaring og kjennskap til sin arbeidsoppgave, vurdere hvordan oppnå forsvarlig sikkerhetsnivå. For risikoanalysen er det naturligvis også gunstig at personell fra sine sektorer gjennomfører risikoanalysen. Det er de som besitter kunnskaper om hva som tidligere har ført til et sikkerhetsbrudd, og hvilke tiltak som er best egnet. Men med silokulturen vil det være utfordrende å skaffe seg det helhetlige bilde av cybersikkerhetstilstanden og følge sikringstiltak og sårbarheter som går på tvers. Dette vil bli enda mer utfordrende ved overgangen til skyløsninger. Ulempene med desentraliseringen er også som det kommer frem fra empirien, at det blir opp til hver ansatt å si hva som er forsvarlig sikkerhet eller ikke. Håndtering av cybersikkerhet må skje både på detaljnivå og på et overordnet nivå. Dette betyr at det fremdeles bør være en risikovurdering som gjelder for hver sektor, men at samme risikovurdering også skal bli gjennomført i hele verdikjeden. Man må kunne kommunisere risikoen på et overordnet nivå for å få et perspektiv på den helhetlige cybersikkerhetstilstanden i NVE. Risiko innenfor det digitale domenet er et dynamisk fenomen som fordrer bedre samstyring og risikokommunikasjon i NVE.

Ifølge Hollnagel (2011) har det tradisjonelle sikkerhetsarbeidet hatt et for snevert utgangspunkt ved kun å ta for seg historiske data. For å kunne si noe om det som kan skje må en også ha en evne til å se på potensielle fremtidige hendelser. I motsetning til det tradisjonelle som begrenser et fremtidsrettet perspektiv ved å analysere feil eller svikt fra tidligere hendelser. Dette prinsippet er relevant for NVE som opererer med en stor organisatorisk og teknisk kompleksitet, hvor det å kartlegge alle potensielle farekilder kan være utfordrende. Resilience Engineerings perspektiv om tilpasningsdyktighet blir sentralt for NVE som blir nødt til å tilpasse seg endringer raskt. Det å kunne styre sikkerhetsarbeidet er ifølge teorien oppnåelig ved å implementere proaktive resilient prosesser som kan håndtere dynamiske situasjoner [49].

Fra empirien kom det frem interessante funn ved å spørre om sårbarheten til cybersikkerheten hos NVE. Informanter ga uttrykk for en ansvarsforskyvning som skjer når det handler om å eie og ha ansvar for dataen sin. Som nevnt spurte en informant «*Hvem eier mail?*», for å illustrere prinsippet om ansvarsforskyvning. Men hvem er det som eier risikoen? I måleverdikjeden er det mange potensielle sårbarheter og risikoer som kan forskyves langs verdikjeden. Men hvem skal ta ansvaret for denne risikoen? Funn fra empirien viser også at det er et ønske om en standard, et rammeverk eller en felles retningslinje for statlige organer for håndtering av cybersikkerhet. Dette blir argumentert for fordi samarbeid mellom statlige organ også kan være med på å heve kompetansenivået for de ansatte i NVE, og til sammen bidra til en tryggere nasjon. Et rammeverk for informasjonssikkerhet kan hjelpe med å forebygge og detektere sikkerhetsbrudd som kompromitterer verdifull informasjon. Rammeverket kan også hjelpe med å avklare tydelige ansvarsroller som har kommet frem som et forbedringspotensial hos NVE. Ifølge informanter er det vanskelig å få ansatte til å ta ansvar for sin data. Ansvaret kan også overføres i verdikjeden for å sikre at leverandører, samt underleverandører har klare ansvarsroller når det gjelder håndtering av cybersikkerhet. Rammeverket kan være løsningen for å tydeliggjøre hvilket ansvar ansatte har for sin data, og gir en felles modell for håndtering av cybersikkerhet som, ifølge informantene er ønsket. Kommunikasjonen kan også lettere skje vertikalt og horisontalt med et rammeverk som gjelder for hele NVE, men også for resten av verdikjeden. Rammeverket kan tilegne en ansvarsrolle som skal være kontaktpersonen for en leverandør og sørge for riktig oppfølgning av den leverandøren. Dersom NVE ikke har tydelige ansvarsroller for hvem som skal følge opp leverandørene kan NVE risikere at leverandører finner «enkle» løsninger som ikke tilfredsstiller sikkerhetskravene. Et eksempel på dette kan være at leverandøren ikke støtter tjenesten Office 365, som NVE benytter seg av i dag. Leverandøren sender beskjed til NVE om integrasjon av tjenesten Office 365, denne ankommer hos en ansatt som ikke har kompetanse innenfor dette fagfeltet og videresender beskjeden. Beskjeden ankommer annen ansatte som har kunnskap om Office 365, men ikke om leverandøren så beskjeden blir videresendt nok en gang. Etter at leverandør har purret på NVE for hjelp med integrasjonen uten at dette lykkes finner de andre løsninger. En annen leverandør tilbyr å installere tjenesten for dem, men denne installasjonen er ikke i henhold til NVEs krav. Som resultat av dette oppstår det et gap mellom intensjon og konsekvens og kan potensielt skape et sikkerhetsbrudd som ingen er klar over.

Med innføring av nok et rammeverk kommer det også utfordringer. Til tross for et beskrivende rammeverk må det foreligge noen spesifikke oppfordringer som tilpasses NVEs ansvarsområder. I rammeverkene NSM har utarbeider benytter de begrepet «forsvarlig sikkerhetsnivå» for å gi rom for fleksibilitet, men virksomheten må selv ha den kompetansen til å vurdere forsvarlig sikkerhetsnivå. Rammeverket er et godt hjelpemiddel for å tydeliggjøre ansvarsroller, eierforholdet til dataen og grad av skjermingsverdig informasjon. Men som med alt annet er det også en bakside ved å utarbeide et rammeverk for håndtering av cybersikkerhet som er offentlig tilgjengelig. Når det er flere statlige organ som følger samme oppskrift vil et angrep som fungerer på en virksomhet lett kopieres og benyttes på flere og deretter spre seg raskt. I prinsippet skal denne fremgangsmetoden være testet av fagpersoner for potensielle sikkerhetsbrudd, hvor en følger en sjekkliste for hvordan testen skal gjennomføres. En faglært person vil i utgangspunktet gå gjennom sjekklisten for å detektere sikkerhetsbrudd. En selvlært hacktivist tenker utenfor boksen, og opptrer mer dynamisk for å finne sikkerhetsbrudd. Dette kan ikke en standard ta hensyn til, og dermed kan dette potensielt føre til at alle som følger standarden har samme feil. Noe en angriper kan avsløre ved å benytte samme metode for alle virksomheter standarden gjelder for. Her må man vurdere hva som er av akseptabel risiko.

7 KAPITTEL: KONKLUSJON

Kapittelet konklusjon er det siste og dermed det avsluttende kapittelet for denne studien. I dette kapittelet kommer de konkluderende funnene til å besvare problemstillingen: *Hvordan kan NVE sikre den digitale og skybaserte måleverdikjeden for fjellskredvarsling?* samt de tilhørende forskningsspørsmålene som er undersøkt gjennom studiens teori, metode, empiri og analyse. Formålet til studien har vært å undersøke hvordan man ivaretar cybersikkerheten ved å implementere digitale målere og skyløsning i måleverdikjeden for fjellskredvarsling hos NVE. Undersøkelsene har i stor grad analysert hvordan dagens måleinfrastruktur og databehandlingen fortsatt kan bevare sin integritet. Dette har blitt fremstilt gjennom en grovanalyse som viser hvordan man kan sikre den digitale og skybaserte måleverdikjeden.

Funn fra studiet viser at informantene har et godt innblikk i hvilken risiko og sårbarhet de har, og kan få fremover. Risikobildet påvirker informantene noe forskjellig, avhengig av informantens posisjon i den digitale verdikjeden. Dagens måleinfrastruktur på den tekniske siden har god redundans, men basert på informantene vil den største risikoen være knyttet til

menneskelige feilhandlinger og mangelfull kunnskap om teknologien. Det er en felles oppfatning at det i dag kommer mer målrettede angrep og at det er en økning av utenlandsk etterretning. I tillegg er det enighet om at flere systemer og mer teknologi vil øke angrepsflaten ytterligere. Menneskelige faktorer er og vil være den største risikoen. Den største sårbarheten er de digitale verdikjedene som i dag er så komplekse, uoversiktlige og transnasjonale at det ikke lengre er mulig å holde en oversikt over alle sårbarheter. Funn fra grovanalysen vedlagt viser at den største risikoen er knyttet til tap av data. Grovanalysen representerer et risikobilde som er subjektivt tolket, og manglende kunnskap om analyseobjektet kan ha medført en betydelig epistemisk usikkerhet knyttet til resultatene. Derfor har det blitt lagt vesentlig tid til å beskrive alle antakelser for å underbygge gyldigheten til analysen, disse ligger vedlagt med analysen. De digitale verdikjedene må kontrolleres og ha kontinuerlig oppfølgning for å kunne opprettholde et forsvarlig sikkerhetsnivå. Fra intervjuene kom det tydelig frem at det ikke var god oppfølgning og kontroll på verdikjedene med eksterne aktører, og at leverandørforhold i stor grad var basert på tillit og ikke konkrete sikringstiltak.

Basert på dokumentanalyse, intervjuene og grovanalysen er det utarbeidet følgende organisatoriske og tekniske sikringstiltak for å sikre den digitale og skybaserte måleverdikjeden for fjellskredvarsling:
Organisatoriske:

- Læring – bevisstgjøre ansatte ved å investere tid og ressurser til å generere og spre kunnskap om teknologien. Kunnskap genereres ved å gjennomføre risikoanalyser, kompetansehevende kurs og testing av teknologi.
- Respondere – rask respons, samt fornuftig respons fordrer en beredskapsplan som integreres inn i styringssystemet. Kunnskap om hvordan ulike hendelser oppfører seg bør også være en del av beredskapsarbeidet, samt en kommunikasjonsplan for verdikjeden slik at nødvendig respons blir spredd til berørte ledd.
- Overvåke – logganalyse, revisjonskontroll av leverandører, oversikt over brukerrettigheter. Konkrete tiltak som sammen skal detektere sikkerhetsbrudd på et tidlig stadium for å hindre eskalering og videre spredning.
- Forutse – kontinuerlige vurderinger og analyser før implementering av ny teknologi, eller ved oppdatering, skal avdekke potensielle sikkerhetsbrudd.
- Redusere interaktiv kompleksitet - ved å holde måleverdikjeden så lokal som mulig.

- Løsne tette koblinger og unngå «lock-in effekt» - ikke skap avhengighetsforhold til proprietære leverandører som gir høye byttekostnader, dette gjør de ved å ikke binde seg for mye til en stor leverandør som f.eks. Microsoft.
- Desentralisert styring hos leverandørene i måleverdikjeden, fordi leverandørene har best kunnskap om risikoen knyttet til sine arbeidsoppgaver. Sentralisert styring for NVE som kontrollerer at leverandørene overholder den desentraliserte styringen. NVE kan benytte metodikken fra Schiefloe (2011) for å vurdere samfunnssikkerhet for å oppnå sentralisert styring.

Tekniske:

- Segregerte nettverk – for å hindre uautoriserte brukere å nå inn til skjermingsverdig informasjon bør det i APIene lages datagrensesnitt i skyen. I tillegg vil det forhindre lateral spredning i nettverket.
- Brukerrestriksjoner – ikke tildel administratorrettigheter til den «vanlige» brukere for å hindre lekkasje av rettigheter og kompromitterte data.
- Logganalyse – for å vite hva som har skjedd og bidrar med å oppdage sikkerhetsbrudd tidlig. Hva som bør logges er eksempelvis unormalt datavolum (kan være en indikasjon på tjenestenektangrep), påloggingsforsøk, unormal aktivitet rundt tilkoblinger.
- Inntrengingstester – for å avdekke eventuelle sårbarheter i infrastrukturen langs måleverdikjeden, dette kravet bør også kommuniseres til leverandører av måleverdikjeden.
- Security by design/security by default for å få oversikt over alle åpne porter i brannmurer, rutere og svitsjer.
- Ende-til-ende kryptering for å sikre kommunikasjonen mellom tjenere og servere i måleverdikjeden, samt bevare integriteten til informasjon.
- Maskingenererte passord for å forhindre den menneskelige feilhandlingen med å lage svake passord.
- To-faktors autentisering for å sikre at autoriserte brukere får tilgang til systemet, og uautoriserte brukere adgangsnekt.

Til slutt anbefales det å utarbeide et overordnet rammeverket for håndtering av cybersikkerhet i måleverdikjeden. Et slikt rammeverk vil kunne være nøkkelen til å opparbeide seg et helhetlig perspektiv for å sikre den digitale og skybaserte måleverdikjeden. Dette

rammeverket må distribueres og kommuniserer med andre offentlige samarbeidspartnere, leverandører og underleverandører for den digitale verdikjeden. Rammeverket alene vil ikke gi ønsket sikkerhetsnivå, men gi en tydeligere ansvars- og risikofordeling i hele verdikjeden og sørge for at informasjon som blir klassifisert som skjermeverdig forblir det uavhengig av leddene. Hvert ledd må fortsatt sørge for at de har nødvendige sikringstiltak som er spesifikke for deres område.

7.1 VIDERE FORSKNING

Scenarioanalyse er et hjelpemiddel man kan benytte for å utvikle gode sikringstiltak på en mer proaktiv måte. Scenarioanalyser eller framsyn som det også kan bli kalt er en mulighet de kan løse dette på. Denne metodikken kan sammenlignes med den tankegangen teorien fra Resilience Engineering ved å være proaktiv og fremtidsrettet. En artikkel[16] skrevet av en nærings-ph.d kandidat tar for seg problematikken rundt reaktive risikoanalyser. Løsningen artikkelen påpeker er å benytte seg av scenarioanalyser, hvor man kan være proaktiv ved å prediktere hvordan en situasjon kan se ut i et hendelsesforløp [59]. Analysen kan også blir brukt til å involvere flere av leverandører og underleverandører, som også er et punkt som videre forskning kan ta for seg.

8 REFERANSER

[1] NOU 2006:6, «Når sikkerheten er viktigst,» Justis- og politidepardementet, Oslo, 2006.

[2] NVE, «Mannen,» 22 10 2019. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/kontinuerlig-overvakede-fjellpartier/mannen/. [Funnet 4 Februar 2020].

[3] NVE, «Om NVE,» Norges vassdrag- og energidirektorat, Oslo, 2020.

[4] M. Røyksund og V. A.K, «Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning,» NVE, Oslo, 2020.

[5] Menon Economics, «Er verdiskaping med data noe Norge kan leve av?,» Menon-Publikasjon nr. 88/2019, 2019.

[6] NOU 2018:14, «IKT-sikkerhet i alle ledd - organisering og regulering av nasjonal IKT-sikkerhet,» Justis- og beredskapsdepartementet , Oslo, 2018.

[7] Nasjonal Sikkerhetsmyndighet, «Sikkerhetsfaglig råd,» NSM, Oslo, 2015.

[8] NVE, «Nasjonal beredskapsplan for fjellskred,» Norges vassdrags- og energidirektorat, Oslo, 2015.

[9] NVE, «Fjellskred - overvåkning og beredskap,» Norges vassdrag- og energidirektorat, Oslo, 2017.

[16] Aakre & Bourmistrov, (2020). *Framsyn som risikoradar*

[10] Microsoft, «Seks ting du kanskje ikke visste om sky,» U.A. [Internett]. Available: https://pulse.microsoft.com/nb-no/business-leadership-nb-no/na/fa2-seks-ting-du-kanskje-ikke-visste-om-sky/. [Funnet 6 Februar 2020].

[11] Kommunal- og moderniseringsdepartementet, «Nasjonal strategi for kunstig interlligens,» Rergjeringen.no, Oslo, 2020.

[12] Nasjonal Sikkerhetsmyndighet, «Grunnprinsipper for IKT-sikkerhet Versjon 2.0,» NSM, Sandvika, 2020.

[13] Lovdata, «Forskrift om tekniske krav til byggverk,» 11 Mai 2018. [Internett]. Available: https://lovdata.no/dokument/SF/forskrift/2017-06-19-840?q=bygg%20teknisk%20forskrift. [Funnet 6 Februar 2020].

[14] Nasjonal Kommunikasjonsmyndighet, «EkomROS 2019: Den digitale grunnmuren,» Nkom, Lillesand, 2019.

[15] Norsk Romsenter, «Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur,» Norsk Romsenter , Oslo, 2013.

[16] NVE, «Satellittbasert radarmåling (SB-InSAR),» 29 01 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/satellittbasert-radarmaling-sb-insar/. [Funnet 20 04 2020].

[17] NVE, «Ekstensometere,» 17 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/ekstensometere/. [Funnet 20 04 2020].

[18] NVE, «Tiltmetere,» 14 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/tiltmetere/. [Funnet 20 04 2020].

[19] J. Hardeng, «Fjellskred,» *Store norske leksikon,* 7 Juli 2019.

[20] N. Spjeldnæs, «Forvitring,» *Store norske leksikon,* 30 Juli 2019.

[21] NVE, «Fare- og risikoklassifisering av ustabile fjellparti,» Norges vassdrag- og energidirektorat, Oslo, 2016.

[22] DSB , «Risikostyring i digitale verdikjeder,» Direktoratet for samfunnsikkerhet og beredskap , Tønsberg, 2020.

[23] Varsom, «Hvordan skjer den daglige overvåkningen og rapporteringen?,» U.Å. [Internett]. Available: https://www.varsom.no/fjellskredovervaking/hvordan-skjer-den-daglige-overvakingen-og-rapporteringen/?ref=mainmenu. [Funnet 22 April 2020].

[24] Cactus Geo AS, «Cactus Web,» Cactus Geo AS, Lier, U.Å.

[25] NORSAR, «Om oss,» U.Å. [Internett]. Available: https://www.norsar.no/om-oss/. [Funnet 22 04 2020].

[26] NORCE, «Satellittfjernmåling,» 21 02 2020. [Internett]. Available: https://www.norceresearch.no/forskningstema/satellittfjernmaling. [Funnet 05 05 2020].

[27] Lisalab', «Ellegi srl,» U.Å. [Internett]. Available: http://www.lisalab.com/home/. [Funnet April 22 2020].

[28] NVE, «Bakkebasert radarmåling (GB-InSAR),» 30 01 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/bakkebasert-radarmaling-gb-insar/. [Funnet 22 04 2020].

[29] Politiets sikkerhetstjeneste, «Nasjonal trusselvurdering 2020,» PST, 2020.

[30] P. M. Schiefloe, «En modell for samfunnssikkerhet,» NTNU/SINTEF, Oslo, 2011.

[31] O. A. Engen, B. I. Kruke, P. H. Lindøe, K. H. Olsen, O. Olsen og K. Pettersen, Perspektiver på samfunnssikkerhet, Oslo: Cappelen Damm Akademisk, 2016.

[32] NTNU, «Informasjonssikkerhet- risikovurdering,» U.Å. [Internett]. Available: https://innsida.ntnu.no/wiki/-/wiki/Norsk/Informasjonssikkerhet+-+risikostyring. [Funnet 24 Januar 2020].

[33] Nasjonal Sikkerhetsmyndighet, «Veileder i verdivurdering av informasjon,» NSM, Sandvika, 2020.

[34] NOU 2015:13, «Digital sårbarhet - sikkert samfunn,» Departementets sikkerhets- og serviceorganisasjon, Oslo, 2015.

[35] M. Rausand og I. B. Utne, Risikoanalyse - teori og metode, Bergen: Fagbokforlaget Vigmostad & Bjørke AS, 2014.

[36] B. Turner, Man-made Disaters, London: Wykeham Science Press, 1978.

[37] Opinion AS, «Mørketallsundersøkelsen 2018 - Informasjonssikkerhet, personvern og datakriminalitet,» Næringslivets Sikkerhetsråd, Oslo, 2018.

[38] Nasjonal Sikkerhetsmyndighet, «NSMs grunnprinsipper for IKT-sikkerhet Versjon 1.0,» NSM, Sandvika , 2017.

[39] National Institute of Standards and Technology, «Framework for Improving Critical Infrastructure Cybersecurity,» NIST, USA, 2018.

[40] European Union Agency for Network and Information Security, «An evaluation framework for cyber security strategies,» ENISA, Hellas, 2014.

[41] European Union Agency for Network and Information Security, «Security Framework for Governmental Clouds,» ENISA, Hellas, 2015.

[42] Digitaliseringsdirektoratet, «Hva sier ISO/IEC 27001?,» Difi, U.Å. [Internett]. Available: https://internkontroll-infosikkerhet.difi.no/hva-sier-isoiec-27001. [Funnet 24 Mars 2020].

[43] H. Bang, «Organisasjonskultur: En begrepsavklaring,» *Tidsskrift for norsk psykologiforening*, pp. 326-336, 2013.

[44] NVE, «Metode for å finne kraftsensitiv informasjon på Internett,» Norges vassdra- og energidirektorat, Oslo, 2019.

[45] J. Reason, Managing the Risk of Organization Accident, England: Ashgate publishing company, 1997.

[46] E. Hollnagel, D. Woods og N. Leveson, Resilience Engineering - Concepts and Percepts, Ashgate Publishing Limited, 2006.

[47] E. Hollnagel, Safety-I and Safety-II, Farnham: Ashgate Publishing Co., 2014.

[48] C. Perrow, Normal accident. Living with High-Risk Technologies, USA: Basic Books, 1984.

[49] E. Hollnagel, J. Pariés, D. D. Woods og J. Wreathall, Resilience Engingeering in Practice: A Guidebook, Ashgate Publishing Limited, 2011.

[50] A. Tjora, Kvalitative forskningsmetoder i praksis, Oslo: Gyldendal Norsk Forlag AS, 2012.

[51] T. Thagaard, Systematikk og innlevelse: En innføring i kvalitative metode. 4 utgave, Bergen: Fagbokforlaget, 2013.

[52] D. I. Jakobsen, Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode. 3 utgave, Kristiansand: Høyskoleforlaget, 2000.

[53] O. Njå, T. Aven og W. Rettedal, «Subjektive probability assignment in QRAs for offshore construction and cessation projects,» Sørco, 1998.

[54] T. Thagaard, «Systematikk og innelvelse. En innføring i kvalitativ metode. 5.utgave,» Bergen, Fagbokforlaget, 2018.

[55] Nasjonal Sikkerhetsmyndighet, «Risiko 2019 - Krafttak for et sikrere Norge,» NSM, Sandvika, 2019.

[56] Wikipedia, «Splunk,» 22 Februar 2020. [Internett]. Available: https://en.wikipedia.org/wiki/Splunk. [Funnet 15 Mai 2020].

[57] Kommunal- og moderniseringsdepartementet , «Én digital offentlig sektor : Digitaliseringsstrategi for offentlig sektor 2019-2025,» Regjeringen.no, Oslo, 2019.

[58] Norfund, «Norfund er utsatt for alvorlig svindel,» Norfund, 13 05 2020. [Internett]. Available: https://www.norfund.no/norfund-er-utsatt-for-alvorlig-svindel/. [Funnet 18 05 2020].

[59] S. Aakre og A. Bourmistrov, «Framsyn som risikoradar,» *MAGMA*, pp. 55-61, Feburar 2020.

[60] M. Whitman og J. Herbert, Management Of Information Securiyt (Sixth Edition), Boston: Cengage Learning, Inc, 2019.

[61] NVE, «Differensiell satellittnavigasjonssystemer (dGNSS),» 14 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/differensiell-satellittnavigasjonssystemer-dgnss/. [Funnet 20 04 2020].

[62] NVE, «Laser måling,» 31 01 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/laser-maling/. [Funnet 20 04 2020].

[63] NVE, «Totalstasjon,» 14 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/totalstasjon/. [Funnet 20 04 2020].

[64] NVE, «Klimastasjon - Meterologiske data,» 14 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/klimastasjon-meterologiske-data/. [Funnet 20 04 2020].

[65] NVE, «Borehullsinstrumentering (DMS),» 14 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/borehullsinstrumentering-dms/. [Funnet 20 04 2020].

[66] NVE, «Geofoner og seismometer,» 14 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/geofoner-og-seismometer/. [Funnet 20 04 2020].

[67] NVE, «Mediabank,» 13 02 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/mediabank/. [Funnet 20 04 2020].

[68] NVE, «Kamera -Overvåking,» 30 01 2020. [Internett]. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/instrumentering/kamera-overvaking/. [Funnet 20 04 2020].

[69] M. E. Porter, Competitive Advantages: Creating and Sustaining Superior Performance, New York: Free Press, 1985.

[70] Lloyd's Register Consulting, «Cybersikkerhet og sikkerhetskritiske kontrollsystemer,» 2016. [Internett]. Available: http://docplayer.me/23294910-Cybersikkerhet-og-sikkerhetskritiske-kontrollsystemer.html. [Funnet 18 Februar 2020].

[71] Lovdata, «Forskrift om sikkerhet og beredskap i kraftforsyningen,» 01 Januar 2019. [Internett]. Available: https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157. [Funnet 6 Februar 2020].

[72] Lovdata, «Lov om nasjonal sikkerhet,» 01 Januar 2019. [Internett]. Available: https://lovdata.no/dokument/NL/lov/2018-06-01-24?q=sikkerhetsloven. [Funnet 6 Februar 2020].

[73] J. Hagen, «Teknologiskifte i energiforsyningen,» Norges vassdrag- og energidirektorat, Oslo, 2015.

[74] N. Azam, «Informasjonssikerhetstilstanden i energiforsyningen,» Norges vassdrag- og energidirektorat , Oslo, 2017.

[75] Digital21, «Digitale grep for norsk verdiskapning - Samlede anbefalinger,» Digital21, Oslo, 2018.

[76] H. Dvergsdal, «Digitalisering,» 28 Oktober 2019. [Internett]. Available: https://snl.no/digitalisering. [Funnet 24 Februar 2020].

[77] Digitaliseringsdirektoratet, «Velkommen til Digitaliseringsdirektoratet!,» 15 Januar 2020. [Internett]. Available: https://www.digdir.no/digitalisering-og-samordning/velkommen-til-digitaliseringsdirektoratet/860. [Funnet 24 Februar 2020].

[78] NVE, «Regulering av IKT-sikkerhet,» Norges vassdrag- og energidirektorat, Oslo, 2017.

[79] T. Aven, W. Røed og H. Wiencke, Risikoanalyse (2.utgave), Oslo: Universitetsforlaget AS, 2008.

[80] T. Aven og O. Renn, Risk Management and Governance: Concept, Guideline and Applications, Heidelberg: Springer Verlag, 2010.

[81] NVE, «NVE tar i bruk nye satellittdata for å overvåke snø, is og flommer,» 31 Januar 2020. [Internett].

[82] Etterretningstjenesten , «Fokus 2020,» E-tjenesten, Lutvann, 2020.

[83] E. Andersen og S. R, «Hva er digitalisering?,» *MAGMA*, pp. 18-24, Mai 2017.

9 VEDLEGG

9.1 VEDLEGG 1: DOKUMENTER

	DOK.NR	TITTEL	UTGIVER	PUBLISERT
STANDARD OG RAMMEVERK	1.1	Security Framework for Governmental Clouds	ENISA	2015
	1.2	Veiledning om tekniske krav til byggverk	Direktoratet for byggkvalitet	2017
	1.3	ISO 31000 Risikostyring – Retningslinjer	Standard Norge	2018
	1.4	NSMs Grunnprinsipper for IKT-sikkerhet. Versjon 2.0	NSM	2020
RAPPORT OG TRUSSELVURDERING	2.1	Fokus	Etterretningstjenesten	2020
	2.2	Risiko	NSM	2020
	2.3	Nasjonal trusselvurdering	PST	2020

INTERNE DOKUMENTER	2.4	Risikostyring i digitale verdikjeder	DSB	2020
	2.5	Risikoanalyse av varslet fjellskred i Åknes	DSB	2016
	2.6	Mørketallsundersøkelsen	NSR	2018
	2.7	Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning	NVE	2020
	2.8	Krisino	NSR	2019
	3.1	Senter for fjellskredovervåkning, Stranda	SVF/NVE	U. Å
	3.2	Skisse for måleinfrastrukturen skredvarsling	SVF/NVE	U.Å
	3.3	Beskrivelse av distribusjon av måledata	SVF/NVE	U. Å
	3.4	Prosedyre for systematisk risikovurdering	NVE	2016

9.2 VEDLEGG 2: BEGREPSAVKLARING

CEO svindel: Defineres som svindel utført ved hjelp av en e-post eller telefon fra personer som utgir seg for å være i ledelsen i virksomheten.

Distributed Denial of service (DDoS): Er et tjenestenektangrep der enheten blir overkjørt av meldinger som overbelaster systemet slik at meldinger som skal sendes ikke blir mottatt av sluttbruker.

Enhet: Er en fysisk enhet, som for eksempel kan være digital måler.

Farekilde: En egenskap, en tilstand eller et forhold som kan lede til en uønsket hendelse.

Forvaltede enheter: En datamaskin som kontrolleres og driftes av virksomheten der sluttbrukere ikke kan endre sikkerhetstilstand.

Jamming: Det oppstår når en satellittnavigasjonsmottaker forstyrres overdøves enten av radiostøy eller et annet sterkere frekvenssignal.

Malware: Er en fellesbetegnelse på skadevare og er sammensatt av ordene «Malicious Software». Denne skadevaren inneholder en ondsinnet programvare som skal lure forbruker til å installere det ondsinnede programmet.

Man-in-the middel: Et angrep der hvor angriperen forandrer den opprinnelige meldingen ved å ta over kontrollen av enheten. Et eksempel kan være målere som blir kompromitterte av en potensiell angriper og angriperen sender tilbake målinger som er misvisende fra realiteten.

Meaconing: Retransmisjon av forsinket signal. Retransmisjon av forsinket signal resulterer i at satellittmottakeren beregner feil posisjonering- og tidsinformasjon.

Phishing: Det å forsøke å få sensitiv informasjon fra en bruker ved å sende e-post eller opprette falsk nettside som ser ekte ut, det er gjerne en kopi av en ekte nettside som nettbank eller påloggingssiden til Facebook.

Spoofing: Et angrep som består av å sende falske meldinger. Utsending av falske signaler har som mål å villede satellittmottakeren til å beregne feilaktig posisjon og feil tidsinformasjon.

9.3 VEDLEGG 3: INTERVJUGUIDER

Intervjuguide nr. 1

Intervju-objekt:	**Virksomhet:** Norges vassdrag- og energidirektorat	**Tema:** Måleinfrastruktur
Nr.	Spørsmål:	
Bakgrunn		
1	Hvilken bakgrunn har du?	
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?	
Rutiner, arbeidsoppgaver, planlegging		
3	Hvilke rutiner har dere for å vedlikeholde målerne og opprettholde (overvåke?) deres tekniske tilstand?	
4	Hvilke kriterier har dere i forhold til plassering av målerne med tanke på fysisk angrep?	
5	Hvilke rutiner har dere for å sørge for riktig opplæring med tanke på kvalitet og produktsikkerhet?	
6	Har dere utarbeidet ulike scenarioer der målesystemene blir utsatt for et rettet cyberangrep? Hva er worst case scenario?	
7	Hvilke risikoanalyser har dere gjennomført for å sikre dere mot cyberangrep på måleinfrastrukturen (eller generelt?)?	
8	Hvordan forsikrer dere at underleverandører ikke tilfører systemet mer sårbarhet? Gjennomføres det testing av utstyr før det implementeres?	
Digitaliseringen		
9	Hvordan jobber dere med å tilpasse dere digitaliseringen? Hvilke muligheter ser dere med digitalisering i NVE? Hva vil gi størst verdi for NVE?	
10	Hva er de største utfordringene dere ser med digitalisering?	
11	Hvilken teknologi benyttes og hvorfor?	
12	Opplever dere at forholdet mellom kunnskap og teknologi blir stadig svakere? I det tilfellet, hvordan sørger dere for å lukke dette kunnskapsgapet?	
13	Hvordan sikrer dere at ny teknologi ikke tilfører mer sårbarhet til NVE?	

14	Hvordan ser trusselbildet ut i dag kontra for 10 år siden? Er det flere hendelser i dag enn det det var da og hvordan imøtekommer dere det nye trusselbildet?
15	Hvordan ser trusselbildet ut om 10 år for NVE?
Målesystemene	
16	Hva er det som skjer med en måleverdi fra den blir registret ute i felt til den er synlig på websiden eller i appen for brukeren?
17	Hvilke systemer og nettverk er verdien innom?
18	Hva er målesystemene avhengige av? Tett koblede systemer som må fungere for at målesystemene skal funke? Andre type ressurser?
19	Hvilke tidligere hendelser som teknisk svikt, menneskelig feil, sikkerhetsbrudd o.l? har dere kartlagt i tilknytning til målesystemene?
20	Hva er det som oppfattes som akseptabel risiko knyttet til målesystemene?
21	Hvilke verdier kan en risikere å skade ved sikkerhetsbrudd på målesystemene?
22	Er det konsekvenser som er av særlig interesse? Hva er de?
23	Hvilke sikringstiltak eksisterer det i dag for å bevare integriteten og tilgjengeligheten til målesystemene?
24	Har sikringstiltakene noen kartlagte svakheter? Hvordan kartlegges integreringsprosessen av nye sikringstiltak?
25	Hvilke sårbarheter har dagens måleinfrastruktur? Hvordan blir disse kartlagt og vurdert i forhold til risiko?
Annet	
	Hvordan kan ny teknologi bidra til å redusere disse sårbarhetene på måleinfrastrukturen? Hvordan vil implementering av ny teknologi for måleinfrastrukturen påvirke sikkerhetsrutiner/tiltak i NVE?

Intervjuguide nr. 2

Intervju-objekt:	**Virksomhet:** Norges vassdrag- og energidirektorat	**Tema:** Overvåkingssenter
Nr.	Spørsmål:	
Bakgrunn		
1	Hvilken bakgrunn har du?	
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?	
Rutiner, arbeidsoppgaver, trusselbildet		
3	Hvilke rutiner har dere for å vedlikeholde målerne og opprettholde (overvåke?) deres tekniske tilstand?	
4	Hvilke kriterier har dere i forhold til plassering av målerne med tanke på fysisk angrep?	

5	Hvilke rutiner har dere for å sørge for riktig opplæring med tanke på kvalitet og produktsikkerhet?
6	Har dere utarbeidet ulike scenarioer der målesystemene blir utsatt for et rettet cyberangrep? Hva er worst case scenario?
7	Hvilke risikoanalyser har dere gjennomført for å sikre dere mot cyberangrep generelt? Hvordan er disse gjennomført?
8	Hvordan forsikrer dere at underleverandører ikke tilfører systemet mer sårbarhet? Gjennomføres det testing av utstyr før det implementeres?
9	Hva er akseptkriteriene til risiko knyttet til måleinfrastrukturen? Hvordan utformer dere akseptkriterier for cyberrisiko relatert til måleinfrastrukturen?
10	Hva anser du som den største trusselen for målesystemene? Hvorfor?
11	Hvordan ser trusselbildet ut i dag kontra for 10 år siden? Er det flere hendelser i dag enn det det var da og hvordan imøtekommer dere det nye trusselbildet?
12	Hvordan ser trusselbildet ut om 10 år for NVE?
Teknologi	
13	Hvilken teknologi anvender dere for varslingssystemene? Hvordan fungerer varslingssystemene?
14	Opplever dere at forholdet mellom kunnskap og teknologi blir stadig svakere? I det tilfellet, hvordan sørger dere for å lukke dette kunnskapsgapet?
15	Hvordan vil implementering av ny teknologi påvirker deres arbeidsoppgaver?
16	Hvordan sikrer dere at ny teknologi ikke tilfører mer sårbarhet til NVE?
17	Er risikoen til teknologien som blir brukt vurdert, og hvordan ble dette gjennomført?
18	Hva er den viktigste funksjonen/rollen til Strands overvåkingssenter?
19	Hvordan blir sikkerhetskulturen opprettholdt ved implementering av ny teknologi?
20	Hvor kommer behovet for å integrere ny teknologi fra (krav fra myndigheter, behov fra interessenter eller interne behov)?
Målesystemene	
21	Hva er det som skjer med en måleverdi fra den blir registret ute i felt til den er synlig på websiden eller i appen for brukeren?
22	Hvilke systemer og nettverk er verdien innom?
23	Hva er målesystemene avhengige av? Tett koblede systemer som må fungere for at målesystemene skal funke? Andre type ressurser (mobilt nettverk, energiforsyning)?
24	Hvilke tidligere hendelser som teknisk svikt, menneskelig feil, sikkerhetsbrudd o.l har dere kartlagt i tilknytning til målesystemene? Hvorfor skjedde det?
25	Er risiko for cyberhendelser vurdert tilknyttet målesystemene?
26	Hvilke verdier kan en risikere å skade ved sikkerhetsbrudd på målesystemene?

27	Er det konsekvenser som er av særlig interesse dersom svikt i måleinfrastrukturen skulle inntreffe? Hva er de?
28	Hvilke sikringstiltak eksisterer det i dag for å bevare integriteten og tilgjengeligheten til målesystemene?
29	Har sikringstiltakene noen kartlagte svakheter? Hvordan kartlegges integreringsprosessen av nye sikringstiltak?
30	Hvilke sårbarheter har dagens måleinfrastruktur? Hvordan blir disse kartlagt og vurdert i forhold til risiko?
31	Hvilken teknologi er det som blir benyttet i måleinfrastrukturen og hvorfor blir dette brukt?
32	Hvordan kan ny teknologi bidra til å redusere eventuelle sårbarheter på måleinfrastrukturen? Hvordan vil implementering av ny teknologi for måleinfrastrukturen påvirke sikkerhetsrutiner/tiltak i NVE?
Annet	
	Føler du at det ikke foreligger nok eventuelt utilstrekkelige retningslinjer for cybersikkerhet for den type virksomhet (ikke helt riktig å si virksomhet, men type arbeidsoppgaver) som dere driver med?

Intervjuguide nr. 3.0

Intervju-objekt:	**Virksomhet:** Norges vassdrag- og energidirektorat	**Tema:** Sikkerhet og sårbarhet
Nr.	Spørsmål:	
Bakgrunn		
1	Hvilken bakgrunn har du?	
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?	
Trusselbildet		
3	Hvordan har trusselbildet endret seg for NVE i løpet av de 5 siste årene?	
4	Hva gjør dere for å imøtekomme det endrede trusselbildet?	
5	Hva anser dere som den største trusselen når informasjon blir mer tilgjengelig for alle?	
6	Hvem utgjør den største trusselen for NVE? Hva er det mest attraktive målet NVE har for en potensiell trusselagent?	
7	Hvilke verdier anses som mer kritisk dersom de skulle blitt kompromittert? Hvordan vurderer dere denne verdien?	
8	Hvor stor del av trusselbildet utgjør det å ha for lite kunnskaper om teknologien som brukes? Eller den menneskelige faktoren?	
Implementering av ny teknologi		
9	Hvilke behov har NVE til implementering av ny teknologi for å imøtekomme potensielt nye krav?	

10	Hvordan er prosessen for utvelgelse av teknologi? Hvilke faktorer er avgjørende for å ta i bruk ny teknologi?
11	Hvilke sikringstiltak har dere allerede installert for å minimere sårbarheten til ny teknologi?
12	Hvordan vil ny teknologi kunne tilføre mer sårbarheten hos NVE?
13	Hvilke IKT-tjenester blir outsourcet i dag? Hvordan kvalitetssikres disse underleverandørene?
14	Blir det brukt multiple sikringstiltak for å skape redundans? Hva er sikringstiltakene (følger samme protokoll, snakker samme språk etc.)?
15	Hvilke vurderinger ligger til grunn for å integrere ny teknologi? Risikovurdering, pentesting etc.
16	Hvordan påvirker ny teknologi sikkerhetskulturen i NVE? Holdninger til ansatte og motivasjon til ny teknologi?
17	Hvordan skal dere sikre tilstrekkelig forståelse og kunnskap til ny teknologi som skal integreres?
Sårbarheter, kartlegging og cyberrisiko	
18	Har NVE oversikt over alle systemer? Gamle og nye systemer kartlagt?
19	Hvordan vurderer dere konsekvens for utilsiktede hendelser?
20	Hvordan vurderer dere konsekvens for tilsiktede hendelser?
21	Hvordan vurderer dere sannsynligheten for utilsiktede hendelser?
22	Hvordan vurderer dere sannsynligheten for tilsiktende hendelser?
23	Hvordan har dere gjennomført risikoanalyse av cybersikkerhet?
24	Hvilke akseptkriterier er det formet for cyberrisiko? Hva er de, og hvordan vet man at dette er godt nok?
25	Hvordan vurderer og følger dere opp at underleverandørene kontinuerlig etterstreber sikkerhetsprosedyrer?
26	Har dere opplevd at leverandør eller underleverandør har blitt utsatt for cyberangrep? Dersom ja, fikk dette konsekvenser for NVE?
27	Hvilke cyberangrep er mest sannsynlig at NVE kommer til å bli utsatt for? Hvordan er dette vurdert, og hvordan er dere forberedt på det?
28	Hva er den største sårbarheten til NVE? Og hva er den hendelsen som flest ganger fører til et sikkerhetsbrudd?
Annet	
29	Føler dere et økende behov for standardiseringer og nettverksløsninger som kan tilpasses flere formål? Ønsker dere mer retningslinjer, krav og veiledninger? Hva er deres tanker rundt mer retningslinjer til cybersikkerhet?

Intervjuguide nr. 3.1

Intervju-objekt:	**Virksomhet:**	**Tema:**
	Norges vassdrag- og energidirektorat	Sikkerhet og sårbarhet

Nr.	Spørsmål:
Bakgrunn	
1	Hvilken bakgrunn har du?
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?
Trusselbildet	
3	Hvordan har trusselbildet endret seg for dere i løpet av de 5 siste årene?
4	Hva gjør dere for å imøtekomme det endrede trusselbildet?
5	Hva anser dere som den største trusselen når informasjon blir mer tilgjengelig? Og den største trusselen med å benytte en skybasert løsning?
6	Hvem utgjør den største trusselen for den kritiske måleinfrastruktur? Hva er det de er ute etter å få tak i?
7	Hvilke verdier anses som mer kritisk dersom de skulle blitt kompromittert? Hvordan vurderer dere denne verdien?
8	Hvor stor del av trusselbildet utgjør det å ha for lite kunnskaper om teknologien som brukes? Eller den menneskelige faktoren?
Implementering av ny teknologi	
9	Hvilke behov har dere til implementering av ny teknologi for å imøtekomme potensielt nye krav?
10	Hvordan er prosessen for utvelgelse av teknologi gjennomført?
11	Hvorfor er det valgt å bruke Splunk og ikke Azure?
12	I forbindelse med skyløsning, hvem er det som eier dataen og hvem er det som har tilgang på dataen? Fører dere noe oversikt over hvem som til enhver tid har tilgang på dataen?
13	Hvilke sikringstiltak har dere allerede installert for å minimere sårbarheten til ny teknologi? Hvordan og hvorfor vil ny teknologi kunne tilføre mer sårbarhet?
14	Hvilke fordeler og ulemper vil det være å ta i bruk skyløsning?
15	Hvordan kan dere kvalitetssikre sømløst samarbeid mellom Splunk og Azure?
16	Hvordan påvirker ny teknologi sikkerhetskulturen hos dere? Holdninger til ansatte og motivasjon til å ta i bruk ny teknologi?
17	Hvordan skal dere sikre tilstrekkelig forståelse og kunnskap til den nye teknologien som skal anvendes?
18	Hvordan vil implementering av ny teknologi påvirke verdikjeden? Nye avhengigheter? Ekstern lagring av data?
Målesystemene og beredskap	
19	Hvilke cyberangrep er målesystemene spesielt utsatt for? Hvordan blir dette kartlagt, vurdert og håndtert?
20	Hva er den største sårbarheten til målesystemene dersom de blir IIoT-enheter? Hvordan er dette vurdert?

21	Hvilke andre leverandører enn NORCE gir måledata til overvåkingssenteret? Hvordan er tjenesten leverandørene gir kvalitetssikret?
22	Hvor mange ledd er måledata gjennom fra digitale målere til den blir publisert på varsom.no? Hvor er det størst sannsynlighet for at måledata kan bli kompromittert i løpet av verdikjeden?
23	Dersom transnasjonal leverandør av måledata, hvordan kan man forsikre at måledata ikke har blitt kompromittert?
24	Hvordan påvirker Splunk sårbarheten til målesystemene? Positivt/negativt?
25	Har det blitt registret hendelser som har ført til svikt i måleinfrastrukturen? Tilsiktede/utilsiktede?
26	Hvilke sikringstiltak har dere for å redusere nedetiden til målesystemene?
27	Hvilke konsekvenser vil et vellykket cyberangrep mot overvåkingssenteret kunne få?
28	Hvilke scenario er worst case for dere? Hvordan er dere forberedt på dette?
Annet	
29	Føler dere et økende behov for standardiseringer og nettverksløsninger som kan tilpasses flere formål? Ønsker dere mer retningslinjer, krav og veiledninger? Hva er deres tanker rundt mer retningslinjer til cybersikkerhet?

Intervjuguide nr. 3.2

Intervju-objekt:	**Virksomhet:** Norges vassdrag- og energidirektorat	**Tema:** Sikkerhet og sårbarhet
Nr.	Spørsmål:	
Bakgrunn		
1	Hvilken bakgrunn har du?	
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?	
Trusselbildet		
3	Hvordan har trusselbildet endret seg for NVE i løpet av de 5 siste årene?	
4	Hva gjør dere for å imøtekomme det endrede trusselbildet?	
5	Hva anser dere som den største trusselen når informasjon blir mer tilgjengelig, og når man tar i bruk mer digitaliserte løsninger?	
6	Hvem utgjør den største trusselen for NVE? Hva er det de er ute etter?	
7	Hvilke verdier anses som mer kritisk dersom de skulle blitt kompromittert? Hva er de? Hvordan vurderer dere denne verdien?	
8	Hvor stor del av trusselbildet utgjør det å ha for lite kunnskaper om teknologien som brukes? Eller den menneskelige faktoren?	
Implementering av ny teknologi og sikringstiltak		
9	Hvilke behov har NVE til implementering av ny teknologi for å imøtekomme potensielt nye krav?	

10	Hvordan er prosessen for utvelgelse av teknologi gjennomført? Hvorfor er det valgt å bruke den teknologien som blir brukt?
11	Hvilke sikringstiltak har dere allerede installert for å minimere sårbarheten til ny teknologi? Hvordan vil ny teknologi kunne tilføre mer sårbarheten hos NVE?
12	Hvilke IKT-tjenester blir outsourcet i dag, hvorfor? Hvordan kvalitetssikres disse underleverandørene, kontinuerlig?
13	Blir det brukt multiple sikringstiltak for å skape redundans? Hva er sikringstiltakene (følger samme protokoll, snakker samme språk etc.)?
14	Hvilke vurderinger ligger til grunn for å integrere ny teknologi? Risikovurdering, pentesting etc.
15	Hvordan påvirker ny teknologi sikkerhetskulturen i NVE? Holdninger til ansatte og motivasjon til ny teknologi?
16	Hvordan skal dere sikre tilstrekkelig forståelse av den nye teknologien som skal anvendes?
Beredskap, kartlegging og cyberrisiko	
17	Hvordan løser man det å være proaktiv på en god måte når det kommer til å beskytte seg mot cyberrisiko?
18	Hvilke system er mest utsatt for angrep? Og hvilke tiltak har blitt gjort for å redusere sannsynligheten for et vellykket angrep?
19	Har dere registret tidligere hendelser innen cyberangrep? Skal man være åpen om det eller holde det for seg selv (innenfor NVE)?
20	Et vellykket angrep er bare et spørsmål om tid, hvordan er dere forberedt på det angrepet?
21	Gjennomfører dere beredskapsanalyser? Hvordan prioriterer dere hvilke hendelser som skal utarbeides beredskapsplaner for?
22	Hva er den mest vanlige menneskelige feilen som fører til sikkerhetsbrudd hos NVE? Hvilke tiltak gjøres for å unngå menneskelig feil?
23	Hva er de mest sannsynlige uønskede hendelsene som kan oppstå for NVE? Tilsiktede og utilsiktede
24	Hvilken skadevare er det som er mest kritisk at NVE blir utsatt for? Hvordan håndterer dere både sannsynligheten for at det skjer og konsekvensen dersom det skjer?
25	Hva er den største risikoen knyttet til leverandører og underleverandører?
26	Hvordan vurderer og følger dere opp at leverandører og underleverandørene kontinuerlig etterstreber NVEs sikkerhetsprosedyrer og krav?
27	Hvordan vurderer dere sannsynligheten for utilsiktede hendelser?
28	Hvordan vurderer dere sannsynligheten for tilsiktende hendelser?
29	Hvordan har dere gjennomført risikoanalyse av cybersikkerhet tidligere?
30	Hvilke akseptkriterier er det utformet for cyberrisiko? Hva er de, og hvordan vet man at dette er godt nok?
Annet	

31	Føler dere et økende behov for standardiseringer og nettverksløsninger som kan tilpasses flere formål? Ønsker dere mer retningslinjer, krav og veiledninger? Hva er deres tanker rundt mer retningslinjer til cybersikkerhet?

Intervjuguide nr. 3.3

Intervju-objekt:	**Virksomhet:** Norges vassdrag- og energidirektorat	**Tema:** Sikkerhet og sårbarhet
Nr.	Spørsmål:	
Bakgrunn		
1	Hvilken bakgrunn har du?	
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?	
Trusselbildet		
3	Hvordan har trusselbildet endret seg for NVE i løpet av de 5 siste årene?	
4	Hva gjør dere for å imøtekomme det endrede trusselbildet?	
5	Hva anser dere som den største trusselen ved å ta i bruk en skybasert løsning?	
6	Hvem utgjør den største trusselen for NVE? Hva er det mest attraktive målet NVE har for en potensiell trusselagent?	
7	Hvilke verdier anses som mer kritisk dersom de skulle blitt kompromittert? Hvordan vurderer dere denne verdien?	
8	Hvor stor del av trusselbildet utgjør det å ha for lite kunnskaper om teknologien som brukes? Eller den menneskelige faktoren?	
Implementering av ny teknologi		
9	Hvilke behov har NVE til implementering av ny teknologi for å imøtekomme potensielt nye krav?	
10	Hvordan er prosessen for utvelgelse av teknologi gjort? Hvorfor er det valgt å bruke den teknologien som blir brukt? Hvilke vurderinger ligger til grunn for å integrere ny teknologi? Risikovurdering, pentesting etc.	
11	I forbindelse med skyløsning, hvem er det som eier dataen og hvem er det som har tilgang på dataen? Fører dere noe oversikt over hvem som til enhver tid har tilgang på dataen?	
12	Hvilke fordeler og ulemper vil det være å ta i bruk skyløsning?	
13	Hvordan kan dere kvalitetssikre sømløst samarbeid mellom Splunk og Azure?	
14	Hvordan sørger dere for at tiltak for å implementere ny teknologi ikke «hemmer» eksisterende tiltak for operativ teknologi?	
15	Hvordan oppstår sårbarheten ved implementering av ny teknologi?	
16	Hvordan påvirker ny teknologi sikkerhetskulturen i NVE? Holdninger til ansatte og motivasjon til ny teknologi?	
17	Hvordan skal dere sikre tilstrekkelig forståelse av den nye teknologien som skal anvendes?	

Sårbarheter, kartlegging og cyberrisiko	
18	Har NVE oversikt over alle systemer? Gamle og nye systemer kartlagt? Overføring av brukerrettigheter?
19	Opplever dere en manglende oversikt over systemene som NVE har, og er alle avhengigheter kartlagt?
20	Hvordan vurderer og følger dere opp at underleverandørene kontinuerlig etterstreber sikkerhetsprosedyrer? Hva er den største risikoen knyttet til leverandører og underleverandører?
21	Har dere registret tidligere hendelser innen cyberangrep? Hva er de mest sannsynlige uønskede hendelsene som kan oppstå for NVE? Tilsiktede og utilsiktede
22	Hvordan vurderer dere sannsynligheten for utilsiktede hendelser? Hvordan vurderer dere sannsynligheten for tilsiktende hendelser?
23	Hvordan har dere gjennomført risikoanalyse av cybersikkerhet tidligere?
24	Hvilke akseptkriterier er det formet for cyberrisiko? Hva er de og hvordan vet man at dette er godt nok?
25	Hvordan holder dere oversikt over adgangskontroller til brukere av systemet? Er det mange adminbrukere?
26	Hvilke rutiner har dere i forbindelse med brukerrettigheter? Fjerning av rettigheter, lekkasje av rettighet ol. Eksternt og internt
27	Hvilket sikkerhetsbrudd ville vært worst case for NVE? Hvordan er dere forberedt på å håndtere dette?
28	Hvordan har dere vurdert lagring av sensitiv informasjon utenfor NVEs kontor i forbindelse med skyløsningen?
Annet	
29	Føler dere et økende behov for standardiseringer og nettverksløsninger som kan tilpasses flere formål? Ønsker dere mer retningslinjer, krav og veiledninger? Hva er deres tanker rundt mer retningslinjer til cybersikkerhet?

Intervjuguide nr. 3.4

Intervju-objekt:	**Virksomhet:** Norges vassdrag- og energidirektorat	**Tema:** Sikkerhet og sårbarhet
Nr.	Spørsmål:	
Bakgrunn		
1	Hvilken bakgrunn har du?	
2	Kan du fortelle litt om hva arbeidshverdagen din går ut på og hvilke ansvarsområder har du?	
Trusselbildet		
3	Hvordan har trusselbildet endret seg for NVE i løpet av de 5 siste årene?	
4	Hva gjør dere for å imøtekomme det endrede trusselbildet?	

5	Hva anser dere som den største trusselen når informasjon blir mer tilgjengelig? Og den største trusselen med å benytte en skybasert løsning?
6	Hvem utgjør den største trusselen for NVE? Hva er det de er ute etter?
7	Hvilke verdier anses som mer kritisk dersom de skulle blitt kompromittert? Hvordan vurderer dere denne verdien?
8	Hvor stor del av trusselbildet utgjør det å ha for lite kunnskaper om teknologien som brukes? Eller den menneskelige faktoren?
Implementering av ny teknologi	
9	Hvilke behov har NVE til implementering av ny teknologi for å imøtekomme potensielt nye krav?
10	Hvordan er prosessen for utvelgelse av teknologi gjort? Hvorfor er det valgt å bruke den teknologien som blir brukt?
11	Hvilke sikringstiltak har dere allerede installert/gjennomført for å minimere sårbarheten til ny teknologi? Hvordan vil ny teknologi kunne tilføre mer sårbarheten hos NVE?
12	Hvilke vurderinger ligger til grunn for å integrere ny teknologi? Risikovurdering, pentesting etc.
13	I forbindelse med skyløsning, hvem er det som eier dataen og hvem er det som har tilgang på dataen? Fører dere noe oversikt over hvem som til enhver tid har tilgang på dataen?
14	Hvordan skal man forsikre seg at samarbeidet mellom Splunk og Azure skjer sømløst? Hvor ligger sårbarheten ved å ta i bruk både Splunk og Azure?
15	Hvilke fordeler og ulemper vil det være å ta i bruk skyløsning?
16	Hvordan vil implementering av skyløsning påvirke verdikjeden? Nye avhengigheter? Ekstern lagring av data?
17	Hvordan påvirker ny teknologi sikkerhetskulturen i NVE? Holdninger til ansatte og motivasjon til å ta i bruk ny teknologi?
18	Har NVE nok kompetanse til å vurdere om en skyløsning er sikker eller ikke til enhver tid?
Sårbarheter, kartlegging og cyberrisiko	
19	Har NVE oversikt over alle systemer? Gamle og nye systemer kartlagt? Brukerrettigheter på gamle systemer, overføres til nye systemer ol.
20	Opplever dere at det er en manglende oversikt over systemene som NVE har, og er alle avhengigheter kartlagt?
21	Ved outsourcing av tjenester, hvordan vurderer og følger dere opp at underleverandørene kontinuerlig etterstreber sikkerhetsprosedyrer som NVE har?
22	Har dere registret tidligere hendelser innen cyberangrep? Hvilke cyberangrep er mest sannsynlig at NVE kommer til å bli utsatt for?
23	Hvordan vurderer dere sannsynligheten for utilsiktede hendelser? Hvordan vurderer dere sannsynligheten for tilsiktende hendelser?
24	Hvordan har dere gjennomført risikoanalyse av cybersikkerhet tidligere?

25	Hvilke akseptkriterier er det formet for cyberrisiko? Hva er de og hvordan vet man at dette er godt nok?
26	Hva er den største sårbarheten/svakheten til NVEs IKT-sikkerhet? Og hva er den hendelsen som flest ganger fører til et sikkerhetsbrudd?
27	Hva er den mest vanlige menneskelige feilen som fører til sikkerhetsbrudd hos NVE? Hvilke tiltak gjøres for å unngå menneskelig feil?
28	Hvilke scenario er worst case for dere? Hvordan er dere forberedt på dette?
Annet	
29	Føler dere et økende behov for standardiseringer og nettverksløsninger som kan tilpasses flere formål? Ønsker dere mer retningslinjer, krav og veiledninger? Hva er deres tanker rundt mer retningslinjer til cybersikkerhet?

9.4 VEDLEGG 4: RISIKOANALYSEN

Informasjon fra intervjuene er brukt til å utarbeide risikoanalysens konsekvenser og sannsynligheter. Informantene nevner kritikaliteten til måledatas tilgjengelighet og integritet noe som legger betydelige føringer for hvordan risikoanalysen vurderes. For sikre den digitale og skybaserte måleverdikjeden er det tatt utgangspunkt i fire ulike uønskede hendelser. De fire uønskede hendelsene som skal analyseres i de tre verdikjedene er:

1. Mister tilgang
2. Ustabil tilgang
3. Tap av data
4. Data er kompromittert

Disse skal bli representert i leddene fra den interne, norske og transnasjonale verdikjeden. Tabellen skal fungere som en forklaring til tallene fremstilt i risikomatrisen.

Sannsynlighetstabell [60]:

Rangering	Beskrivelse	Sannsynlighet	Frekvens
1.	Svært lite sannsynlig	5% sannsynlig å skje i løpet av de neste 12 månedene	Kan skje en gang i løpet av 20 år (Det er en ukjent hendelse som ikke er kjent enda)
2.	Lite sannsynlig	25% sannsynlig å skje i løpet av de neste 12 månedene	Kan skje en gang i løpet av en 10 år (Det er en potensiell hendelse, som en ikke kjenner til har inntruffet)
3.	Sannsynlig	50% sannsynlig å skje i løpet av de neste 12 månedene	Kan skje en gang i løpet av en 5 års (Det er en kjent hendelse, men som ikke har inntruffet)
4.	Meget sannsynlig	75% sannsynlig å skje i løpet av de neste 12 månedene	Kan skje en gang i løpet av året (Hendelsen har inntruffet enten i Norge eller utlandet)
5.	Svært sannsynlig	100% sannsynlig å skje i løpet av de neste 12 månedene	Garantert å skje opptil flere ganger i løpet av ett år (Hendelsen er kjent)

Konsekvenstabell [35]:

Rangering	Beskrivelse	Konsekvens
1	Ufarlig	Hendelsen vil ikke medføre økonomiske tap for virksomheten, eller påvirke anseelse og integriteten til skredvarslingstjenesten.
2	Lite farlig	Hendelsen kan medføre økonomiske tap for virksomheten (men som kan gjenopprettes) eller føre til mindre tap av tillit til skredvarslingstjenesten.

3	Farlig	Hendelsen kan medføre betydelig økonomiske tap for virksomheten (men som kan gjenopprettes), samt vesentlig tap av anseelse og integritet til skredvarslingstjenesten. Tap av skjermingsverdig informasjon kan være skadelig for tilgjengeligheten til skredvarslingstjenesten.
4	Kritisk	Hendelsen fører til betydelige eller uopprettelige økonomiske tap for virksomheten (og eventuelle leverandører), og kan føre til tap av liv og helse for tredjepart. Tap av skjermingsverdig informasjon kan føre til vesentlig økt sårbarhet for integriteten og tilgjengeligheten for skredvarslingstjenesten.
5	Katastrofalt	Hendelsen fører til konsekvenser som påvirker tillit til organisasjonen som helhet, i form av betydelig/uopprettelig økonomiske tap, eller tap av anseelse og integritet til skredvarslingstjenesten, samt tap av liv og helse for tredjepart. Tap av skjermingsverdig informasjon kan føre til vesentlig økt sårbarhet for organisasjonen.

9.4.1 INTERN VERDIKJEDE

Ledd: Sensor

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
1	Mister tilgang	-Værforhold - Interferens - Manglende vedlikehold av måleinstrument - Skjerming - Romvær - Fiberbrudd - Fysisk ødeleggelse av måleinstrument -Strømbrudd -Offentlige IP-adresser	Overvåkingssenteret får ikke tilgang på sanntidsdata til å gjøre løpende vurdering av risikoutsatte fjellparti. Ødelagte måleinstrument må erstattes og gir økonomiske konsekvenser, samt tap av verdifull måledata.	-Overvåker tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen -Hvert målesystem har sin unike strømkilde for å unngå dominoeffekt	4	2	8	-Vedlikehold av måleinstrument -Bedre fysisk sikring av måleinstrument -Robuste fiberkabler
2	Ustabil tilgang	- Interferens - Tjenestenekt - Værforhold - Skjerming av signaler -Manglende sikkerhetsoppdatering	Ustabil tilgang fører til at posisjonering og tidsaspektet blir misvisende som gjør det vanskeligere å vurdere den faktiske tilstanden.	-IDS -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	5	1	5	-Robuste innretninger -Pen-testing -Patching
3	Tap av data	-Åpne porter i nettverket -Strømbrudd -Fysisk ødeleggelse av måleinstrument -Manglende risikovurdering	Overvåkingssenteret får ikke kritiske måledata som gir utslag på vurderingsgrunnlaget til videre analyse av ustabile fjellparti.	-Overvåking tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	3	5	15	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument
4	Data er kom-promittert	-Åpne porter i nettverket -Tilkobling på måleinstrument -Manglende deteksjonssystem -Interferens	Uautoriserte bruker får tilgang på måledata, som kan fører til måledata mister sin integritet.	-Teknisk personell og geologer vurderer validiteten til måledata	3	3	9	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument -Opplæring av personell

Ledd: Bunker i fjellet

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
5	Mister tilgang	-Værforhold -Strømbrudd -Slitasje på fiberkabler	Overvåkingssenteret får ikke tilgang på sanntidsdata til å	-Overvåking av værforhold -Vedlikehold av utstyr	4	1	4	-Ekstern strømkilde -Whitelist

		-Programvarefeil -Fiberbrudd -Svitsjer ramler ut -Rutere mister signal	gjøre løpende vurdering av risikoutsatte fjellparti.	-Lagrer data selv om den ikke oversendes direkte				-Programvare-oppdatering
6	Ustabil tilgang	-Værforhold -Interferens -Tjenestenekt via DNS på over 100 Gbps	Ustabil tilgang fører til at posisjonering og tidsaspektet blir misvisende som gjør det vanskeligere å vurdere den faktiske tilstanden.	-IDS -Overvåking av værforhold -Vedlikehold av utstyr -Overvåking av tilstand til måleinstrument	4	1	4	-Pen-testing -Logganalyse -VPN-programvare -Patching
7	Tap av data	-Fysisk ødeleggelse av feltpc -Åpne porter i ruter/svitsjer -Strømbrudd -Ukryptert trådløs aksesspunkt -Tap av ekstern strømkilde	Overvåkingssenteret får ikke måledata som gir utslag på vurderingsgrunnlaget til videre analyse av ustabile fjellparti.	-Overvåking av værforhold -Vedlikehold av utstyr -Overvåking av tilstand til måleinstrument -Oversikt over åpne porter i ruter -Måleinstrument med sin unike strømkilde gir redundans -VPN	2	5	10	-Bedre fysisk sikring av utstyr -Ruter og svitsjer som støtter WPA-kryptering -Oversikt over trådløse aksesspunkt -Kryptere trådløse aksesspunkt
8	Data er kom-promittert	-Utnyttelse av dårlig Wi-Fi ruter kryptering (WEP) -Åpne porter i ruter/svitsjer -Manglende IDS -Ikke-forvaltede enheter (private mobiler)	Uautoriserte bruker får tilgang på måledata, som fører til måledata mister sin integritet og kan føre til følgefeil for videre beslutninger.	-IDS -Opplæring -Vurdere alltid teknologi før den blir implementert for å minimere sårbarhet	2	2	4	-Kontinuerlig sjekk av åpne porter i ruter og svitsjer -Ruter og svitsjer som støtter WPA-kryptering

Ledd: Stranda/Ekstern lagring

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
9	Mister tilgang	-Fiberbrudd -Interferens -Værforhold -Phishing fører til at autorisert bruker ikke får tilgang -Datainnbrudd -Manglende oversikt over sårbarhet -Programvarefeil	Ansatte får ikke mulighet til å gjøre jobben sin som følge av at de ikke har tilgang på data, gir negative følgeeffekt for skredvarslingen.	-Vedlikehold av utstyr -Overvåking av værforhold og måleinstrument -Segregert nettverk -To-faktors autentisering	3	4	12	-Beredskapsplan -Whitelist -Fysisk sikring av data og sikkerhetskopi -Risikoanalyse over sårbarheter -Prosedyrer for
10	Ustabil tilgang	-Tjenestenekt via DNS på over 100 Gbps	Kan føre til at måledata mister sin integritet da	-IDS	3	2	6	-Oversikt over alle forvaltede og ikke-

		-Interferens -Manglende dekning -Gammel teknologi -Manglende sikkerhetsoppdatering -Medbragt ikke-forvaltede enheter	posisjon og tidsaspektet kan være påvirket som følge av interferens.	-Maskinvare som tåler stor belastning -Kontinuerlig oppdatering -Segregert nettverk				forvaltede enheter som påkobles segregert nettverk -Logganalyse
11	Tap av data	-Åpne porter i brannmur -Manglende risikovurderinger - Innsider -Manglende sikkerhetskopi -Manglende forståelse av Splunk -Menneskelige feilhandlinger -Manglende autentisering av grensesnitt	Nåtidens analyse, men også fremtidige analyser, påvirkes som følge av tap av måledata. Dette vil få ringvirkninger til den kritiske samfunns-funksjonen skredvarsling som følge av manglende beslutnings-grunnlag.	-Oversikt over alle åpne porter i brannmuren (security by default) -Restriksjoner av brukerrettigheter -Ekstern lagring av sikkerhetskopi	3	5	15	-Beredskapsplan -Bevisstgjøring av ansatte -Logganalyse
12	Data er kom-promittert	-DNS-kapring som følge av ruter konfigurert etter fjernadministrasjon -Overføring med mobildata blir utsatt for Menneske-i-midten angrep -Sårbarheter i Wi-Fi-kryptering -Medbragt ikke-forvaltede enheter -Manglende kunnskap om utvikling av datadelingsgrensesnitt	-Finner ruterens grensesnitt og kaprer brukerens nettverkstrafikk -Data blir avlyttet og mister sin integritet - Avlytter Wi-Fi-trafikk mellom aksesspunkt og klient	-Kryptert Wi-Fi tilkobling -Segregert nettverk -VPN-kryptering	3	4	12	-Flere DNS-servere -Ende-til-ende kryptering -Oversikt over alle forvaltede og ikke-forvaltede enheter som påkobles segregert nettverk -Sikker konfigurering av on-premis løsning -API med autentisering

Ledd: Regionalt kontor NVE

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
13	Mister tilgang	-Datainnbrudd -Phishing fører til at autorisert bruker ikke får tilgang -Manglende oversikt over sårbarhet -Strømbrudd	Ansatte får ikke tilgang på systemer som fører til økonomiske tap, samt stans i distribusjon av måledata.	-Stillestående oversikt over systemer -Kurs på cybersikkerhet	3	3	9	-Beredskapsplaner -Opplæring av ansatte -Et levende dokument over aktive systemer i NVE
14	Ustabil tilgang	-Interferens -Tjenestenekt via DNS på over 100 Gbps -Medbragt ikke-forvaltede enheter	Måledata fra leverandør kan være kompromittert og interferens kan forårsake	-IDS -Oversikt over åpne porter i brannmur (Security by default)	5	1	4	-Maskinvare som tåler stor belastning over tid

		-Manglende sikkerhetsrutiner -Manglende oversikt over tillatte programmer -Feil i Proxy-server	forsinket overføring av måledata.	-Opplæring av ansatte				-Whitelist for tillatte program -Flere DNS servere -Pen-testing -Reinstallere Proxy-server
15	Tap av data	-Mangelfulle risikovurderinger -Manglede sikkerhetskopi som følge av skyløsningens lagringsprosedyre -Innsider -Manglende selskapsgjennomgang av skyleverandør -Manglende oversikt over grensesnitt -Åpne kildekode program (frigir kode for en type lisens)	Avhengighet til skyleverandør fører til at NVE ikke har kompetanse til å ha løpende vurdering hvorvidt data er trygt oppbevart eller ikke. Leverandør har også mulighet til å påkoste økonomiske påkjenninger for at NVE skal være sikre på at data blir forsvarlig oppbevart.	-Risikovurdering av skyleverandør -Risikovurdering for lagring av data hos skyleverandør -Ekstern strømkilde -Sikkerhetskopi -Brannmur	4	4	16	-Løpende vurdering av skyleverandør -Vurdere å benytte flere ulike tjenester fra ulike skyleverandør for å minimere avhengighet til en leverandør, men må holde oversikt
16	Data er kom-promittert	-Feil tilgangsstyring av data -Menneskelig svikt -Manglende opplæring -Svake passord -API installert uten autentifikasjon	Uautoriserte brukere får tilgang til skjermingsverdig informasjon, samt eskalere brukerrettigheter for å ta seg videre inn i nettverket.	-Opplæring av ansatte -Brannmur -Bevisstgjøring av ansatte	4	3	12	-Beredskapsplan -Øvelser -Pen-testing -Maskingenererte passord

Ledd: Publisering

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
17	Mister tilgang	-Manglende oversikt over brukerrettigheter -Tap av ekstern kraft -Anvender gammel teknologi	Varslingsportalen varsom.no blir utilgjengelig som hindrer NVE å opplyse befolkningen om farenivåer for skredutsatte fjellparti.	-IDS -Ekstern strømkilde -Opplæring av ansatte -Oversikt over system (ikke et levende dokument)	2	3	6	-Kontinuerlig oppdatering -Dynamisk oversikt over system og systembrukere -Tekniske barrierer for å minimere menneskelige feilhandlinger
18	Ustabil tilgang	-Tjenestenekt via DNS på over 100 Gbps -Interferens -IP-kapring -Datavirus -Ny teknologi	Teknisk personell og geologer får ikke publisert oppdatert informasjon på varslingsportalen.	-IDS -Opplæring av ansatte -Vurdering av ny teknologi før det tas i bruk	4	2	8	-Tilpasset maskinvare som tåler stor belastning -Kontinuerlig øvelser og bevisstgjøring av aktuelle trusler

		-Menneskelige feilhandlinger						-Test av teknologi før implementasjon
19	Tap av data	-Lekkasje av brukerrettigheter -Innsider fjerner tilsiktet eller utilsiktet data -Manglende etterlevelse av lover og regler	Data som gir grunnlaget til informasjon som publiseres er borte, slik at det fører til brudd på den kritiske samfunnsfunksjonen varslingstjenesten.	-Restriksjoner til brukerrettigheter -Sikkerhetskopi -Oversikt over åpne porter i brannmur (security by default)	3	5	15	-Logganalyse av brukere - Kryptert ekstern sikkerhetskopi -Logging av brannmur og tjenester
20	Data er kom-promittert	-Dårlige passord -Manglende oversikt over autoriserte brukere -Utilstrekkelig segregering av nettverk -Menneskelige feilhandlinger -Manglende prosedyre for håndtering av skjermingsverdig informasjon	Informasjon som blir publisert på varsom.no kan være misvisende og føre til at mennesker stoler på oppgitt informasjon og følgelig oppbevarer seg i skredutsatte område.	-Restriksjoner for brukerrettighet -Oversikt over åpne porter i brannmur (security by default)	3	4	12	-Maskin-genererte passord som oppbevares forsvarlig -Ende-til-ende kryptering -Bevisstgjøring av ansatte

Risikobildet før implementerte sikringstiltak:

Konsekvens / Sannsynlighet	1. Ufarlig	2. Lite farlig	3. Farlig	4. Kritisk	5. Katastrofalt
5.Svært sannsynlig	*2,14*				
4. Meget sannsynlig	*5,6*	*1,18*	*16*	*15*	
3. Sannsynlig		*10*	*4,13*	*9,12,20*	*3,11,19*
2. Lite sannsynlig		*8*	*17*		*7*
1.Svært lite sannsynlig					

Etter implementerte sikringstiltak:

Konsekvens / Sannsynlighet	1. Ufarlig	2. Lite farlig	3. Farlig	4. Kritisk	5. Katastrofalt
5.Svært sannsynlig					
4. Meget sannsynlig	**1,5,14**		**15**		
3. Sannsynlig	**2,6,18**	**10,13,16**	**12**		**11,19**
2. Lite sannsynlig		**4,8,17**	**9**	**7**	**3,20**
1.Svært lite sannsynlig					

Ledd: Sensor (Felles for alle måleverdikjedene)

1. *Mister tilgang*: Konsekvensen av å miste tilgang kan reduseres ved å benytte andre metoder for å overføre data på enn fiberkabler da disse er ansett som skjøre innretninger. Sannsynligheter vil derimot forbli den samme da det vil være utfordrende å gjøre noe med ekstremvær som fører til tap av signal og mister tilgang av den grunn.

2. ***Ustabil tilgang***: Man reduserer sannsynligheten for at en mister tilgang ved å benytte seg av robuste måleinstrumenter med god fysisk sikring, samt gjennomføre testing i form av penetrasjonstester og patching for å avdekke sikkerhetshull. Konsekvensen for å miste tilgang er ansett som ufarlig da måledata ikke blir borte med lagret til tross for at signalet er borte, så personell kan hente ut måledata når signalet er oppe igjen.
3. ***Tap av data*****:** Tap av måledata er kritisk og vil være kritisk dersom det skulle forekomme i leddet sensor da det ikke har mulighet til å bli gjenopprettet, derfor vil konsekvensen forbli den samme. Sannsynligheten for tap av data kan dog bli redusert som følge av oversikt til eventuelle porter som kan være åpne for uautoriserte brukere å lukke disse. Fysisk sikring for å hindre ondsinnede handlinger mot måleinstrumentene vil også kunne bidra til å redusere sannsynligheten for tap av data**.**
4. ***Kompromittert data*****:** Kompromittert måledata kan ved hjelp av fagpersoner bli vurdert som legitime eller ikke som kan redusere konsekvensen som å stole på misvisende verdier. Sannsynligheten for at det skjer kan også bli redusert som følge av at man er klar over alle porter som er åpne i nettverket som kan utnyttes av uautoriserte brukere.

Ledd: Bunkers i fjellet
5. ***Mister tilgang***: Ved hjelp av ekstern strømkilde og holde oversikt over godkjente programvarer som kan nedlastet er det mulig å redusere sannsynligheten for at en mister tilgang til utstyret i bunkeren. Det vil være lite farlig å miste tilgang til bunkers i fjellet for her lagres data dersom signalet ikke fungerer for å unngå noe tap av data.
6. ***Ustabil tilgang***: Man kan redusere konsekvensen fra farlig til lite farlig ved å gjennomføre penetrasjonstester som viser sårbarheter til nettverket i bunkeren. Dette gjør at man kan implementere tiltak som kan minske konsekvenser for at måledata viser feilaktig posisjonering og tidsaspekt.
7. ***Tap av data*****:** Tap av måledata er katastrofalt, men sannsynligheten kan reduseres dersom man finner gode nok forebyggende tiltak. Bedre fysisk sikring vil gjøre det mer robust for tilsiktede og utilsiktede å påvirke måleinfrastrukturen. En oversikt over alle mulige porter som kan være åpne for den uautoriserte bruker vil også kunne hjelpe for å redusere sannsynligheten for at noen kan fjerne kritisk måledata.
8. ***Kompromittert data***: Kompromittert data vil kunne bli kvalitetssikret hos personell som har mulighet til å legitimere integriteten til måledata for å redusere konsekvensen.

Ledd: Stranda/Ekstern lagring
9. ***Mister tilgang*****:** Man kan redusere konsekvensen ved å miste tilgang på overvåkingssentret ved å ha en prosedyre klar der hvor man vet hvordan en skal håndtere en slik situasjon, og hvilke tiltak en skal gjøre for å gjenopprette normalsituasjon. En risikoanalyse over sårbarheter overvåkingssenteret kan være hensiktsmessig for å avdekke sårbarheter som kan føre til en situasjon der man mister tilgang.
10. ***Ustabil tilgang*****:** Konsekvensene til ustabil tilgang hos overvåkingssentret kan reduseres ved å ha restriksjoner for medbragte ikke-forvaltede enheter som forstyrrer signaler, eller kaster ansatte ut av nettverket. Logganalyse kan også være behjelpelig for å kunne logge all aktivitet som kan føre til ustabil tilgang for å redusere sannsynlighet for at det skjer.
11. ***Tap av data*****:** Tap av måledata vil være katastrofalt for både nåtidens situasjon, men man mister også grunnlaget for fremtidige predikasjoner. Men sannsynligheten kan derimot reduseres ved å være bevisst om oppbevaring og håndtering av kritiske måledata, logganalyse kan også avdekke aktivitet som kan føre til tap av data.
12. ***Kompromittert data*****:** Sannsynlighet til å få kompromittert data kan reduseres ved å implementere ende-til-ende kryptering som gjør det vanskelig for en uautorisert bruker å kompromittere informasjonen ved overføringer.

Ledd: Regionalt kontor NVE (felles for alle måleverdikjedene)
13. ***Mister tilgang*****:** Konsekvensen av å miste tilgang på regionalt kontor hos NVE vil kunne påvirkes ved å ha segregert nettverk for å hindre lateral spredning til andre virksomheter, dersom uautorisert bruker skulle ta seg inn via en ansatt som har fått frastjålet sine bruker-kredentialer. Sannsynlighet kan også reduseres ved å ha et levende dokument som viser alle aktive systemer i NVE.
14. ***Ustabil tilgang*****:** Sannsynligheten kan reduseres ved å anskaffe maskinvare som tåler stor belastning over tid for å hindre at tjenestenektangrep skal påvirke trafikken på nett til tross for at mange ansatte er inne i systemet.

15. *Tap av data*: Ved skyløsninger må man behandle lagring av data på en annen måte, og ved tap av data er det vanskelig å gjøre noen konsekvensreduserende tiltak for at dataen skal kunne bli gjenopprettet. Sannsynligheten kan derimot bli redusert ved grundig vurdering av skyleverandør for å forsikre seg om hvordan prosessen for oppbevaring av data er i henhold til NVEs krav til forsvarlig oppbevaring.
16. *Kompromittert data*: Konsekvensen vil vedvare som kritisk selv etter implementert sikringstiltak, men sannsynlighet for at det skjer kan reduseres ved å ha avanserte passord, gjennomføre penetrasjonstester, og utarbeide beredskapsplan for å hindre eskalering av den uønskede hendelsen.

Ledd: Publisering (felles for alle måleverdikjedene)
17. *Mister tilgang*: Ved å gjennomføre kontinuerlig sikkerhetsoppdateringer og holde oversikt over brukerrettigheter til enhver tid vil det være mulig å redusere sannsynligheten for at en mister tilgang. Tekniske barrierer vil kunne redusere konsekvensen av menneskelige feilhandlinger som kan begrense skaden dersom det skulle skje.
18. *Ustabil tilgang*: Sannsynligheten kan reduseres ved å implementere maskinvare som tåler stor belastning over tid, samtidig som ansatte er observante og bevisste på mistenkelig aktivitet for å unngå. Ny teknologi må også testet inn i et lignede system før det blir implementer for å unngå sårbarheter som ny teknologi kan medføre.
19. *Tap av data*: Tap av data vil kunne bli gjenopprettet da dette er siste ledd av en verdikjede så det vil være mulig å tilbakeføre data, men det vil kunne påvirke varslingsportalens funksjonalitet da den ikke vil være oppdatert på grunn av manglende data. Konsekvens og sannsynlighet for at dette skjer vil vedvare til tross for sikringstiltak, dette grunnet innsideren som er meget vanskelig å være forvente når det skjer eller hva som er målet.
20. *Kompromittert data*: Det vil være vanskelig å redusere konsekvensene dersom data som er publisert er kompromittert dersom uautorisert bruker har tilegnet kontroll over nettportalen varsom.no. Det er lite sannsynlig at dette kommer til å skje, men ikke usannsynlig, fordi det er umulig å vite om alle sårbarheten som kan utnyttes av andre.

9.4.2 EKSTERN NORSK VERDIKJEDE

Ledd: Sensor

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
1	Mister tilgang	- Værforhold - Interferens - Manglende vedlikehold av måleinstrument - Skjerming - Romvær - Fysisk ødeleggelse av måleinstrument - Strømbrudd	Overvåkingssenteret får ikke tilgang på sanntidsdata til å gjøre løpende vurdering av risikoutsatte fjellparti. Ødelagte måleinstrument må erstattes og gir økonomiske konsekvenser.	-Overvåker tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen -Hvert målesystem har sin unike strømkilde for å unngå dominoeffekt	4	2	8	-Vedlikehold av måleinstrument -Deteksjonssystem -Bedre fysisk sikring av måleinstrument -Robuste fiberkabler
2	Ustabil tilgang	- Interferens - Tjenestenekt via DNS på over 100 Gbps - Værforhold - Skjerming av signaler -Romvær	Ustabil tilgang fører til at posisjonering og tidsaspektet blir misvisende som gjør det vanskeligere å vurdere den faktiske tilstanden.	-Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	5	1	5	-Deteksjonssystem -Robuste innretninger
3	Tap av data	-Manglende fysisk sikring av måleinstrument -Åpne porter i nettverket	Overvåkingssenteret får ikke kritiske måledata som gir utslag på vurderingsgrunnlaget	-Overvåking tilstand til måleinstrument	3	5	15	-Oversikt over åpne porter i nettverket

		-Strømbrudd -Manglende risikovurdering	til videre analyse av ustabile fjellparti.	-Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen				-Bedre fysisk sikring av måleinstrument
4	Data er kom-promittert	-Åpne porter i nettverket - Tilkobling på måleinstrument -Manglende deteksjonssystem	Uautoriserte bruker får tilgang på kritiske måledata, som fører til måledata mister sin integritet.	-IDS -Teknisk personell og geologer vurderer validiteten måledata	3	3	9	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument

Ledd: NORSAR/NORCE

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
5	Mister tilgang	-Strømbrudd -Menneskelige feilhandlinger -Manglende deteksjonssystem -Ukryptert trådløs aksesspunkt	Ekstern leverandør får ikke hentet ut måledata for å bearbeide og prosessere informasjon videre.	-IDS -Restriksjoner til brukerrettigheter -Opplæring -Brannmur	2	3	6	-Ekstern strømkilde -Bevisstgjøring av forsvarlig IKT-sikkerhet - VPN-kryptering
6	Ustabil tilgang	-Tjenestenekt via DNS på over 100 Gbps - Gammel teknologi snakker ikke med ny teknologi -Manglende dekning -Interferens -Feil i protokoll TCP/IP -Svitsjer med fabrikatinnstilling	Nettverkstrafikk fra svitsjer med fabrikatinnstilling kan bli publisert på svitsjen og fører til at mange i NORSAR/NORCE får ustabil tilgang.	-Maskinvare som tåler stor belastning -IDS -Vurdering av teknologi før implementasjon (security by design)	4	2	8	-IDS -Testing av teknologi før implementasjon -Kontinuerlig oppdatering -Reinstallere protokoll TCP/IP
7	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data -Ukryptert trådløs aksesspunkt -Åpne porter i nettverket -Manglende sikkerhetsoppdatering -Manglende risikovurdering -Åpne porter i brannmuren	Mister kritiske måledata til å vurdere tilstand til risikoutsatte fjellparti.	-Restriksjoner til brukerrettigheter -Sikkerhetskopi -IDS -Oversikt over åpne porter i brannmur (security by default)	3	5	15	-Logganalyse -Ekstern sikkerhetskopi hos leverandør -Opplæring -Prosedyre for fjerning av brukerrettighet
8	Data er kom-promittert	-Åpne porter i brannmuren -Ukryptert kommunikasjon fra måleinstrument til dataserver -Innsider lekker informasjon -Dårlige passord	Ekstern leverandør får tilgang til sensitiv informasjon og kan ta seg videre inn i nettverket. Skjermingsverdig informasjon blir distribuert/endret slik at	-Inngått avtale med leverandør som skal overholde krav -Lukket nettverk for å hindre lateral spredning -VPN-konto	4	4	16	-Løpende kontroll av leverandør -Tydeliggjøre sikkerhetskrav -Logganalyse

			informasjon mister sin integritet.					-Restriksjoner for brukerrettigheter

Ledd: Pronoia/EPOS-N

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå S	K	RPN	Anbefalt tiltak
9	Mister tilgang	-Nettverksbrudd -Phishing fører til at autorisert bruker ikke får tilgang -Medbragte ikke-forvaltede enheter -Dårlige passord -Manglende kartlegging av avhengighet til leverandør	Ikke-forvaltede enheter kan være infisert av trojaner eller virus som ønsker å spre seg til andre enheter, stor spredning inn i nettet kan føre til et botnet tjenestenektangrep.	-Ekstern strømkilde -E-post filtrering -Segregert nettverk -Opplæring	4	4	16	-Beredskapsplan -Bevisstgjøring for behandling av e-post -Restriksjoner for medbragte ikke-forvaltede enheter -Maskingeneret passord
10	Ustabil tilgang	-Tjenestenekt via DNS på over 100 Gbps -Interferens -Menneskelige feilhandlinger -Ustabil DNS-server	Redusert kapasitet på nettverket kan potensielt forårsake at server krasjer dersom det vedvarer og lengre tid. Ustabil tilgang vil også gjøre det vanskelig å få distribuert oppdatert informasjon.	-IDS -Opplæring	3	2	6	-Flere DNS-servere -Maskinvare som tåler stor belastning over tid (minimum 60 minutter) -Patching -Pen-testing
11	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data -Menneskelige feilhandlinger -Manglende oversikt over brukerrettigheter	Historiske data og sanntidsdata som er nødvendig for videre analyse svekker beslutningsgrunnlag for beredskapsnivået tilknyttet risikoutsatte fjellparti.	-Sikkerhetskopi -Opplæring -Restriksjoner for brukerrettigheter	2	5	10	-Logganalyse -Begrenset antall som har fjernrettigheter -Bevisstgjøring av hvordan oppbevare data forsvarlig
12	Data er kom-promittert	-Lekkasje av brukerrettigheter -Manglende tilgangsstyring -Feil i kopifelt til e-post -Tailgating	Skjermingsverdig informasjon blir distribuert/endret til uautorisert bruker slik at informasjon mister sin integritet.	-VPN-konto -Lukket nettverk -Oversikt over systembrukere -Teknisk personell og geologer kan vurdere validitet til måledata.	4	3	12	-Logganalyse -Bevisstgjøring av ansattes behandling av mail -To-faktors autentisering ved ankomst til bygg (biometrisk og PIN-kode)

Ledd: Regionalt kontor NVE

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå S	K	RPN	Anbefalt tiltak

13	Mister tilgang	-Manglende risikovurdering av anvendt teknologi -Tap av ekstern kraft -Phishing fører til at autorisert bruker ikke får tilgang	Uautorisert bruker kan ta seg inn i nettverket fjerne autorisert brukers tilgang og kompromittere skjermeverdig informasjon.	-Restriksjoner for brukerrettigheter -Sikkerhetskopi -Bevisstgjøring av potensielle trusler for ansatte	3	3	9	-Gjennomføre risikovurdering jevnlig -Ekstern strømkilde -Opplæring og bevissthet om bruk av e-post
14	Ustabil tilgang	-Organisatoriske endringer fra leverandør -Menneskelige feilhandlinger -Feil i Proxy-server	Måledata fra leverandør kan være kompromittert og interferens kan forårsake forsinket overføring av måledata.	-Inngått avtale om krav med leverandør -IDS	4	1	4	-Bevisste om endringer fra leverandør -Kurs og opplæring av ansatte -Reinstallere Proxy-server
15	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data uten sikkerhetskopi -Menneskelige feilhandlinger fører til tap av data -Mangelfulle risikovurderinger -Manglende etterlevelse av lover, regler og interne krav -Tailgating -Manglende grensesnitt i dataisolasjonen	Kritisk måledata eller annen skjermeverdig informasjon som er nødvendig for å kunne anslå beredskapsnivået til risikoutsatte fjellparti borte, slik at det vil kunne påvirke fremtidige og nåtidens situasjon.	-Ekstern strømkilde -Sikkerhetskopi -Restriksjon til brukerrettighet for fjerning av data -Ansvarliggjøring av leverandør -To-faktors autentifisering	4	4	16	-Prosedyre for å fjerne rettigheter for brukere -Opplæring og bevissthet om håndtering av data -Ekstern lagring av sikkerhetskopi -Grundig løpende vurdering av leverandører
16	Data er kom-promittert	-Manglende risikovurdering av leverandør -Manglende segregering av nettverk -Manglende sletting av data -Due diligence -Manglende autentisering av API	Uautoriserte brukere kan eskalere brukerrettigheter som kan føre til lateral spredning i nettverket. Skjermingsverdig informasjon kan bli distribuert med uautoriserte brukere.	-Brannmur -Sektorbasert verdivurdering (vurdering er sektorbasert)	4	3	12	-Segregert nettverk for å hindre spredning -Verdivurdering for skjermeverdig informasjon på et overordnet nivå

Ledd: Publisering

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
17	Mister tilgang	-Tap av ekstern kraft -Dekningsfeil -Menneskelige feilhandlinger -Manglende deteksjonssystem -Manglende kartlegging av avhengigheter til leverandør	Varslingsportalen varsom.no blir utilgjengelig som hindrer NVE å opplyse befolkningen om farenivåer for skredutsatte fjellparti.	-IDS -Ekstern strømkilde -Opplæring av ansatte -Oversikt over system (ikke et levende dokument)	2	3	6	-Kontinuerlig oppdatering -Dynamisk oversikt over system og systembrukere -Tekniske barrierer for å minimere menneskelige feilhandlinger

18	Ustabil tilgang	-Interferens -Tjenestenekt via DNS på over 100 Gbps -Menneskelige feilhandlinger -Feil i protokoll TCP/IP -Manglende oversikt over sårbarheter til leverandører	Teknisk personell og geologer får ikke publisert oppdatert informasjon på varslingsportalen.	-IDS -Opplæring av ansatte	4	2	8	-Maskinvare som tåler stor belastning over tid (minimum 60 minutter) -Kontinuerlig øvelser og bevisstgjøring av aktuelle trusler -Reinstallere protokoll TCP/IP
19	Tap av data	-Manglende risikovurdering -Manglende sikkerhetsoppdatering -Innsider utfører tilsiktet eller utilsiktet fjerning av data -Organisatoriske endringer hos skyløsningen Azure	Data som gir grunnlaget til informasjon som publiseres er borte, slik at det fører til brudd på den kritiske samfunnsfunksjonen varslingstjenesten.	-Restriksjoner til brukerrettigheter -Sikkerhetskopi -Oversikt over åpne porter i brannmur (security by default)	3	5	15	-Logganalyse av brukere - Kryptert ekstern sikkerhetskopi -Logging av brannmur og tjenester
20	Data er kom-promittert	-Lekkasje av brukerrettigheter -Mangelfull tilgangsstyring -Utilstrekkelig segregering av nettverk	Informasjon som blir publisert på varsom.no kan være misvisende og føre til at mennesker stoler på oppgitt informasjon og følgelig oppbevarer seg i skredutsatte område.	-Restriksjoner for brukerrettighet -Oversikt over åpne porter i brannmur (security by default)	3	4	12	-Maskin- genererte passord som oppbevares forsvarlig -Ende-til-ende kryptering

Risikobildet før implementerte sikringstiltak:

Konsekvens / Sannsynlighet	1. Ufarlig	2. Lite farlig	3. Farlig	4. Kritisk	5. Katastrofalt
5.Svært sannsynlig	*2*				
4. Meget sannsynlig	*14*	*1,6,18*	*12,16*	*8,9,15*	
3. Sannsynlig		*10*	*4,13*	*20*	*3,7,19*
2. Lite sannsynlig			*5,17*		*11,20*
1.Svært lite sannsynlig					

Etter implementerte sikringstiltak:

Konsekvens / Sannsynlighet	1. Ufarlig	2. Lite farlig	3. Farlig	4. Kritisk	5. Katastrofalt
5.Svært sannsynlig					
4. Meget sannsynlig	**1,14**	**16**	**15**		
3. Sannsynlig	**2,18**	**6,10,12**	**8,9**	**7**	**19**
2. Lite sannsynlig		**4,17**	**5,13**	**11**	**3,20**
1.Svært lite sannsynlig					

Ledd: NORSAR/NORCE
5. Mister tilgang: Det vil generelt være vanskelig å redusere sannsynligheten og konsekvenser for menneskelige feilhandlinger, samtidig som å beskytte måleinstrument for å bli utsatt for ekstremvær er ansett som for kostbart.
6. Ustabil tilgang: Ved deteksjonssystem og testing av teknologi vil man kunne redusere sannsynligheten for at NORSAR/NORCE opplever ustabil tilgang.
7. Tap av data: Ved å utføre logganalyse, ha ekstern sikkerhetskopi ved en annen sted kan man redusere konsekvensen til tap av data. Sannsynligheten vil forbi grunnet den manglende kompetansen til å forebygge innsideren.
8. Kompromittert data: Løpende kontroll av leverandører vil kunne redusere sannsynligheten for at data blir kompromittert. Tydeliggjøring av sikkerhetskrav, restriksjoner for brukerrettigheter sammen med logganalyse vil bidra til å redusere konsekvensene for data som blir kompromittert.

Ledd: Pronoia/EPOS-N
9. Mister tilgang: Sannsynligheten for å miste tilgang kan reduseres ved å innføre restriksjoner på ikke-forvaltede enheter (private mobiler o.l.). Konsekvensen kan reduseres ved å utarbeide en beredskapsplan for hvordan en lengre nedetid skal håndteres raskt for å gjenopprette normaltilstand raskest mulig.
10. Ustabil tilgang: Sannsynligheten og konsekvensen vil forbli den samme grunnet den manglende kunnskapen til å beskytte seg mot alle menneskelige feilhandlinger.
11. Tap av data: Logganalyse, restriksjoner for brukerrettigheter kan være med på å redusere konsekvensene for tap av data. Samtidig som ansatte bevisstgjøres på hvordan skjermingsverdig informasjon skal oppbevares for å unngå menneskelige feilhandlinger.
12. Kompromittert data: To-faktors autentisering bidrar til å redusere sannsynligheten for at data blir kompromittert. I tillegg vil bevisstgjøring av ansattes vurdering av e-post være en barriere for å hindre at data blir kompromittert.

9.4.3 EKSTERN TRANSNASJONAL VERDIKJEDE

Ledd: Sensor

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
1	Mister tilgang	-Værforhold - Interferens - Manglende vedlikehold av måleinstrument - Skjerming - Romvær - Fiberbrudd - Fysisk ødeleggelse av måleinstrument -Strømbrudd	Overvåkingssenteret får ikke tilgang på sanntidsdata til å gjøre løpende vurdering av risikoutsatte fjellparti. Ødelagte måleinstrument må erstattes og gir økonomiske konsekvenser, samt tap av verdifull måledata.	-Overvåker tilstand til måleinstrument -Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen -Hvert målesystem har sin unike strømkilde for å unngå dominoeffekt	4	2	8	-Vedlikehold av måleinstrument -IDS -Bedre fysisk sikring av måleinstrument -Robuste fiberkabler
2	Ustabil tilgang	- Interferens - Tjenestenekt via DNS på over 100 Gbps - Værforhold - Skjerming av signaler	Ustabil tilgang fører til at posisjonering og tidsaspektet blir misvisende som gjør det vanskeligere å vurdere den faktiske tilstanden.	-Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen	5	1	5	-IDS -Robuste innretninger
3	Tap av data	-Åpne porter i nettverket -Strømbrudd	Overvåkingssenteret får ikke kritiske måledata som gir	-Overvåking tilstand til måleinstrument	3	5	15	-Oversikt over åpne porter i nettverket

		-Fysisk ødeleggelse av måleinstrument -Manglende risikovurdering	utslag på vurderingsgrunnlaget til videre analyse av ustabile fjellparti.	-Flere måleinstrument på samme fjellparti gir redundans i infrastrukturen				-Bedre fysisk sikring av måleinstrument
4	Data er kom-promittert	-Åpne porter i nettverket -Tilkobling på måleinstrument -Manglende deteksjonssystem	Uautoriserte bruker får tilgang på kritiske måledata, som fører til måledata mister sin integritet.	-Teknisk personell og geologer vurderer validiteten til måledata	3	3	9	-Oversikt over åpne porter i nettverket -Bedre fysisk sikring av måleinstrument -IDS

Ledd: Italia

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
5	Mister tilgang	-Tjenestenekt via DNS på 100 Gbps -Key-loggers får kontoopplysning og endrer passord -Ekstremvær -Programvarefeil	Ekstern leverandør får ikke hentet ut måledata for å bearbeide og prosessere informasjon videre.	-VPN-konto -Inngått avtale med leverandør som skal overholde krav	2	3	6	-Secure DNS -Tilpasset maskinvare som tåler stor belastning -Kontinuerlig oppdateringer
6	Ustabil tilgang	-Interferens -Noen applikasjoner snakker ikke med eksisterende teknologi -Manglende oppdatering	Sanntidsdata mister sin verdi da posisjon og tidsaspektet blir misvisende i forhold til måledata.	-VPN-konto -Inngått avtale med leverandør som skal overholde krav	4	3	12	-IDS -Testing av teknologi før implementasjon -Kontinuerlig oppdatering -Restriksjoner på skjermingsverdig informasjon
7	Tap av data	-Dårlige passord eller dårlig oppbevaring av passord -Manglende rutine for lagring av ulike data -Utilfredsstillende sikring av data	Mister kritiske måledata til å vurdere tilstand til risikoutsatte fjellparti.	-VPN-konto -Andre måleinstrument kan fortsatt gi data -Inngått avtale med leverandør som skal overholde krav	3	5	15	-Bevissthet rundt oppbevaring og vanskelighetsgrad til passord -Sikkerhetskopi -Krav til oppbevaring av data -Løpende vurdering av leverandør
8	Data er kom-promittert	- Manglende etterlevelse av lover, regler og interne krav -Utilfredsstillende oppbevaring av data	Måledata mister sin integritet og skjermingsverdig infrastruktur kan bli påvirket som følge av misvisende måledata.	-Inngått avtale med leverandør som skal overholde krav -Lukket nettverk for å hindre lateral spredning	4	4	16	-Løpende kontroll av leverandør -Tydeliggjøre sikkerhetskrav -Logganalyse -Ende-til-ende kryptering

Ledd: NVE server i Oslo

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
9	Mister tilgang	-Manglende deteksjonssystem -Mangelfull tilgangsstyring -Maskinvarefeil -Programvarefeil i brannmur -Datainnbrudd -Manglende oppfølgning av skyløsningen	Uautoriserte brukere kan benytte stjålet enheter til å utnytte den ansattes identitet som kan føre til tap av viktige verdier og/eller tilgang på viktige tjenester som blir gjort utilgjengelig.	-IDS -Restriksjoner til brukerrettigheter -Opplæring -Brannmur	3	4	12	-Fysisk sikring av serverpark -To-faktor autentisering -Logganalyse -Whitelisting
10	Ustabil tilgang	-Programvare snakker ikke samme språk -Interferens -Tjenestenekt via DNS på over 100 Gbps -Feil i Proxy-server -Defekt DNS-server -Feil i protokoll TCP/IP -Manglende oppfølgning av skyløsningen	Redusert kapasitet på nettverket kan potensielt forårsake at server krasjer dersom det vedvarer og lengre tid. Ustabil tilgang vil også gjøre det vanskelig å få distribuert oppdatert informasjon.	-Oversikt over alle systemer -IDS	3	3	9	-Oversikt over alle tilkoblede enheter -Logganalyse -Maskinvare som tåler stor belastning -Ha flere DNS-servere tilgjengelig -Reinstallere protokoll TCP/IP
11	Tap av data	-Mangelfull tilgangsstyring -Manglende segregering av nettverk -Manglende sikkerhetsoppdatering -Innsider -Manglede sikkerhetskopi som følge av skyløsningens lagringsprosedyre -Datainnbrudd	Historiske data og sanntidsdata som er nødvendig for videre analyse svekker beslutningsgrunnlag for beredskapsnivået tilknyttet risikoutsatte fjellparti.	-Brannmur -Oversikt over brukerrettigheter -Opplæring -Inngått avtale med ekstern leverandør	4	5	20	-Beredskaps-plan -Fysisk sikring av lokasjon til server -Ekstern lagring av data -Kvalitetssikre skyleverandørs rutine for oppbevaring av data
12	Data er kom-promittert	-Manglende risikovurdering av leverandør - Manglende krav til leverandør -Utilfredsstillende oppbevaring av data fra leverandør	Uautoriserte brukere kan eskalere brukerrettigheter som kan føre til lateral spredning i nettverket. Data mister sin integritet.	-VPN -Kryptert trådløst aksesspunkt(?)	3	4	12	-Innsiktsrapport -Logganalyse -Ende-til-ende kryptering -Krav til leverandør for oppbevaring av data

Ledd: Regionalt kontor NVE

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
13	Mister tilgang	-Innsider fra leverandør har gjort tjenesten utilgjengelig -Phishing fører til at autorisert bruker ikke får tilgang -Manglende oversikt over systembrukere	Uautorisert bruker kan ta seg inn i nettverket fjerne autorisert brukers tilgang og kompromittere skjermeverdig informasjon.	-Restriksjoner for brukerrettigheter -Sikkerhetskopi -Bevisstgjøring av potensielle trusler for ansatte	3	3	9	-Logganalyse -E-post filtrering -Øvelser -Beredskapsplan

14	Ustabil tilgang	- Organisatoriske endringer fra leverandør -Interferens -Manglende deteksjonssystem -Feil i protokoll TCP/IP	Måledata fra transnasjonal leverandør kan være kompromittert og interferens kan forårsake forsinket overføring av måledata.	-Inngått avtale om krav med leverandør -IDS	4	2	8	- Kvalitetssikre leverandør løpende -Logganalyse -Reinstallere protokoll TCP/IP
15	Tap av data	-Strømbrudd som følge av målrettet angrep mot strømkilde -Innsider fjerner tilsiktet eller utilsiktet data uten sikkerhetskopi -Manglende etterlevelse av lover, regler og interne krav -Tailgating	Kritisk måledata eller annen skjermeverdig informasjon som er nødvendig for å kunne anslå beredskapsnivået til risikoutsatte fjellparti borte, slik at det vil kunne påvirke fremtidige og nåtidens situasjon.	-Ekstern strømkilde -Sikkerhetskopi -Restriksjon til brukerrettighet for fjerning av data -Ansvarliggjøring av leverandør -To-faktors autentifisering	4	5	20	-Beredskapsplan -Ekstern sikkerhetskopi -Krav til oppbevaring av data -Løpende kvalitetssikring av leverandør
16	Data er kom-promittert	-Manglende verdivurdering av skjermeverdig dokumenter -Manglende sletting av data -Ukrypterte trådløse aksesspunkt	Uautoriserte brukere kan eskalere brukerrettigheter som kan føre til lateral spredning i nettverket. Skjermingsverdig informasjon kan bli distribuert med uautoriserte brukere.	-Brannmur -Sektorbasert verdivurdering (vurdering er sektorbasert)	4	3	12	-Segregert nettverk for å hindre spredning -Verdivurdering for skjermeverdig informasjon på et overordnet nivå

Ledd: Publisering

Nr	Risiko-element	Årsak	Konsekvens	Eksisterende sikringstiltak	Risikonivå			Anbefalt tiltak
					S	K	RPN	
17	Mister tilgang	-Manglende oversikt over systembrukere -Strømbrudd som følge av ekstremvær -Manglende oppdatering -Menneskelige feilhandlinger -Mangelfulle risikovurderinger	Varslingsportalen varsom.no blir utilgjengelig som hindrer NVE å opplyse befolkningen om farenivåer for skredutsatte fjellparti.	-IDS -Ekstern strømkilde -Opplæring av ansatte -Oversikt over system (ikke et levende dokument)	2	3	6	-Kontinuerlig oppdatering -Dynamisk oversikt over system og systembrukere -Tekniske barrierer for å minimere menneskelige feilhandlinger
18	Ustabil tilgang	-Interferens -Tjenestenekt via DNS på over 100 Gbps -Menneskelige feilhandlinger -Mangelfull kartlegging av sårbarheter til leverandører	Teknisk personell og geologer får ikke publisert oppdatert informasjon på varslingsportalen.	-IDS -Opplæring av ansatte	4	2	8	-Maskinvare som tåler høy kapasitet -Kontinuerlig øvelser og bevisstgjøring av aktuelle trusler
19	Tap av data	-Innsider fjerner tilsiktet eller utilsiktet data uten sikkerhetskopi	Data som gir grunnlaget til informasjon som publiseres er	-Restriksjoner til brukerrettigheter	3	5	15	-Logganalyse av brukere

		-Åpne porter i brannmuren som lar uautorisert IP-adresse tilgang til systemet -Manglende brukeropplæring	borte, slik at det fører til brudd på den kritiske samfunnsfunksjonen varslingstjenesten.	-Sikkerhetskopi -Oversikt over åpne porter i brannmur (security by default)				- Kryptert ekstern sikkerhetskopi -Logging av brannmur og tjenester
20	Data er kom-promittert	-Svake passord -Manglende oversikt over brukerrettigheter -Åpne porter i brannmuren -Manglende brukeropplæring	Informasjon som blir publisert på varsom.no kan være misvisende og føre til at mennesker stoler på oppgitt informasjon og følgelig oppbevarer seg i skredutsatte område.	-Restriksjoner for brukerrettighet -Oversikt over åpne porter i brannmur (security by default)	2	5	10	-Maskin- genererte passord som oppbevares forsvarlig -Ende-til-ende kryptering

Risikobildet før implementerte sikringstiltak:

Konsekvens / Sannsynlighet	1. Ufarlig	2. Lite farlig	3. Farlig	4. Kritisk	5. Katastrofalt
5.Svært sannsynlig	*2*				
4. Meget sannsynlig		*1,14,18*	*6,16*	*8*	*11,15*
3. Sannsynlig			*4,10,13*	*9,12*	*3,7,19*
2. Lite sannsynlig			*5,17*		*20*
1.Svært lite sannsynlig					

Etter implementerte sikringstiltak:

Konsekvens / Sannsynlighet	1. Ufarlig	2. Lite farlig	3. Farlig	4. Kritisk	5. Katastrofalt
5.Svært sannsynlig					
4. Meget sannsynlig	**1,14**			**11,15**	
3. Sannsynlig	**2,18**	**6,13,16**	**9,10**	**7,8**	**19**
2. Lite sannsynlig		**4,17**	**5,12**		**3,20**
1.Svært lite sannsynlig					

Ledd: Italia

5. Mister tilgang: Det vil være vanskelig å redusere sannsynligheten for at ekstremvær fører til mistet tilgang. Konsekvensene vil heller ikke kunne bli redusert som følge av sikringstiltak grunnet usikkerheten knyttet til ekstremvær.

6. Ustabil tilgang: Prosedyre for kontinuerlig oppdatering vil kunne redusere sannsynligheten for ustabil tilgang. Deteksjonssystemer vil også kunne forhindre at systemet blir tatt ned av store datavolum. Konsekvensen kan reduseres ved å ha restriksjoner på hvilken informasjon som skal deles.

7. Tap av data: Konsekvensen for å miste data kan reduseres ved å implementere krav til leverandører for hvordan data trygt skal oppbevares. I tillegg til å ha en løpende kontroll fra leverandøren.
8. Kompromittert data: Sikkerhetskrav til leverandøren kan hjelpe på å redusere sannsynligheten for at data blir kompromittert. Samt vil ende-til-ende kryptering sørge for at kommunikasjonen er sikker.

Ledd: NVE server i Oslo
9. Mister tilgang: Ved å ha fysisk sikring av serverparken og ved hjelp av to-faktors autentisering kan man redusere sannsynligheten for å miste tilgang. Whitelisting vil også bidra til å vise hvilke programvarer man skal få lov til å laste ned.
10. Ustabil tilgang: Det vil være vanskelig å redusere sannsynlighet og konsekvens for data lagret i skyløsningen, man er ifølge informanter nødt til å stole på Microsoft.
11. Tap av data: Ved å ha kontroll på hvordan data blir fysisk sikret, samt en ekstern lagring av data lokalt vil man kunne redusere konsekvensene for tap av data.
12. Kompromittert data: Innsiktsrapport fra leverandører kan redusere sannsynligheten for at data blir kompromittert. Ende-til-ende kryptering kan redusere konsekvensene og dermed sikre integriteten til informasjonen som sendes.

9.4.4 FORKLARING FOR VURDERING AV SANNSYNLIGHET OG KONSEKVENS

Felles antakelser for intern, norsk og transnasjonal måleverdikjede.

NR	Dokumentanalyse	Intervju	Sannsynlighet	Konsekvens
1	Dok.nr 2.2. Fra Allvis NOR sin tjeneste som NSM tilbyr kom det inn at av 1140 886 så var det 13240 av de som hadde offentlige IP adresser, noe som tilsvarer 1,16%. Dok.nr 2.6 sier at 6% av 1500 virksomheter ble utsatt for dataskadeverk.	Informant A og B sier at fjellparti er utstyrt med multiple måleinstrument, dersom mistet tilgang på en så kan man få måledata fra andre måleinstrument. Informantene sier også at måleinstrumentene er plassert på utsatte områder for ekstremvær.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som lite farlig. Karakter = 2
2	Dok.nr. 2.6 sier at 7% av virksomheter ble utsatt for tjenestenektangrep i året 2017. Videre sier rapporten at 4 til 10 av kundene blir utsatt for tjenestenekt i løpet av en måned.	Informant D sier at geologiske og tekniske personell har mulighet til kvalitetssikre dersom måledata skulle vært kompromittert.	Hendelsen vurderes som svært sannsynlig. Karakter = 5	Hendelsen vurderes som ufarlig. Karakter = 1
3	Dok.nr. 2.2. sier at trusselaktører leter etter sårbare servere, brannmurer, rutere og svitsjer. Disse blir utnyttet til å omgå tekniske sikringstiltak.	Informant A og B sier det er kritisk å miste måledata, men per dags dato ikke opplevd tilsiktet fysisk ødeleggelse av måleinstrumentene.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som katastrofalt. Karakter = 5
4	Dok.nr 1.4 sier at virksomheter ofte har manglende oversikt over hvor egne kabler går og om uvedkommende har fysisk adgang.	Informant A sier at man må ha 100% kontroll på dataen, og at back up måledata blir speilet til annen plass på VMV server, dersom et angrep mot overvåkingssenteret skulle skje.	Hendelsen vurdert til sannsynlig. Karakter = 3	Hendelsen er vurdert til farlig. Karakter = 3
13	Dok.nr. 2.6 sier at 21 % av virksomhetene undersøkt ble utsatt for malware i 2017.	Informant C sier at det er mye lettere å oppdage om man er hacket, men at menneskelige feilhandlinger skjer fordi angrepene er så avanserte.	Hendelsen er vurdert som sannsynlig. Karakter = 3	Hendelsen er vurdert som farlig. Karakter = 3
14	Dok.nr 1.4 sier at virksomheter har liten til ingen kontroll på ikke-forvaltede enheter, utsatt for å bli kompromittert.	Informant C sier at ny teknologi som skal ha mye tilgang, feks. Har telefon har god sikring hos NVE med egne VPN-kontoer og at man krypterer fra oppstart av ny teknologi.	Hendelsen er vurdert som svært sannsynlig. Karakter = 5	Hendelsen er vurdert som ufarlig. Karakter = 1
15	Dok.nr 2.2 sier at man må foreta risikovurdering før implementering fordi lagring av data utenfor Norge innebærer en betydelig risiko.	Informant G sier at kontornettet har flere svakheter og flere muligheter som potensielle trusselaktører kan utnytte. Informant D sier at implementering av skytjeneste fordrer mye bedre håndtering av verdikjeden.	Hendelsen er vurdert som meget sannsynlig. Karakter = 4	Hendelsen er vurdert som kritisk. Karakter = 4
16	Dok.nr 2.6 sier at en av de fire mest vanlige årsakene til sikkerhetsbrudd i 2016 var menneskelige feilhandlinger.	Informant C sier at folk fremdeles har dårlige passord og at man ikke kan stole på at mennesker unngår å gjøre feil.	Hendelsen er vurdert som meget sannsynlig. Karakter = 4	Hendelsen er vurdert som farlig. Karakter = 3
17	Dok.nr 2.2 sier at man må foreta risikovurdering før implementering fordi lagring av data utenfor Norge innebærer en betydelig risiko.	Informant F sier at risikoen for å gjøre feil kommer til å øke betraktelig ved implementering av skyløsning.	Hendelsen er vurdert som lite sannsynlig. Karakter = 2	Hendelsen er vurdert som farlig. Karakter = 3
18	Dok.nr. 2.6 sier at 21 % av virksomhetene undersøkt ble utsatt for malware i 2017.	Informant F sier at man daglig blir utsatt for angrep, typiske løsepengevirus og phishing.	Hendelsen er vurdert som meget sannsynlig. Karakter = 4	Hendelsen er vurdert som lite farlig. Karakter = 2

19	Dok.nr. 2.3 sier at datanettverks-operasjoner utgjør en betydelig trussel for Norge, hvor rekruttering av innsidere gjør at man kan få tilgang til lukkede nettverk.	Informant E sier; desto flere systemer desto større blir angrepsflaten.	Hendelsen er vurdert som sannsynlig. Karakter = 3	Hendelses er vurdert som katastrofalt. Karakter = 5
20	Dok.nr. 2.3 sier at målrettede angrep i form av e-poster fortsatt er aktuelt fordi menneskelige feilhandlinger åpner opp mulighetene ved å klikke på vedlagte linker eller lignende.	Informant F sier at dokumentet for kategorisering av skjermingsverdig informasjon er et sovende dokument og ikke blitt oppdatert.	Hendelsen er vurdert som sannsynlig. Karakter = 3	Hendelsen er vurdert som kritisk. Karakter = 4

Intern verdikjede

NR	Dokumentanalyse	Intervju	Sannsynlighet	Konsekvens
5	Dok.nr 3.3 viser at overføring av måledata skjer via fiberkabel og trådløst.	Informant B forteller at svitsjer faller ut, men som informant A sier vil data bli lagret til tross for mistet tilgang.	Hendelse vurdert til meget sannsynlig. Karakter = 4	Hendelsen vurdert til ufarlig. Karakter = 1
6	Dok.nr 2.2 sier at i tidsrommet 2018 og 2019 ble det ved flere anledninger slått ut GPS-signal som følge av interferens	Informant A sier ved tap av signal vil man få beskjed, og kan hente ut data fra bunker når signalet er oppe igjen for å gjenopprette data.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som ufarlig. Karakter = 1
7	Dok.nr. 1.4 sier at ukryptert kommunikasjon kan føre til brudd på konfidensialitet og integritet. Eller krypteringsnøkler med svak beskyttelse.	Informant A og B sier at måleinstrument har egne fuelcell, strømaggregat og flere ulike måleinstrument på samme fjellparti. Men ved totalt strømbrudd vil måledata gå tapt, og være kritisk for skredvarslingstjenesten.	Hendelsen vurderes som lite sannsynlig. Karakter = 2	Hendelsen vurderes som katastrofal. Karakter = 5
8	Dok.nr 1.4 sier at virksomheter har liten til ingen kontroll på ikke-forvaltede enheter, utsatt for å bli kompromittert.	Informant B sier at det er vanskelig å holde oversikt over alle åpne porter.	Hendelsen vurdert som lite sannsynlig. Karakter = 2	Hendelsen vurdert som lite farlig. Karakter = 2
9	Dok.nr 1.4 sier programvare som implementeres kan inneholde utilsiktede sårbarheter og utgjør en risiko. Dok.nr 2.8 sier at av 2500 private og offentlige virksomheter ble 15% utsatt for svindel i form av løsepengevirus og 13% direktørsvindel.	Informant A sier at måledata blir speilet for ekstern lagring, men at de aldri har fått testet et scenario hvor man mister tilgang som følge av et målrettet angrep.	Hendelsen er vurdert som sannsynlig. Karakter = 3	Hendelsen er vurdert som kritisk. Karakter = 4
10	Dok.nr 1.4 sier at virksomheter har liten til ingen kontroll på ikke-forvaltede enheter, utsatt for å bli kompromittert.	Informant D sier at geologiske og tekniske personell har mulighet til å kvalitetssikre dersom måledata skulle vært kompromittert. Informant A sier at VPN skaper dårlig dekning, og at dagens datalogging krever mye vedlikehold.	Hendelsen vurdert som sannsynlig. Karakter = 3	Hendelsen vurdert som lite farlig. Karakter = 2
11	Dok.nr 2.2 sier at en stor andel virksomheter hadde mangler knyttet til gjennomføring av risikovurderinger.	Informant A sier at det ikke har blitt utført noen skriftlige risikovurderinger for IKT-sikkerhet. Informant A sier at de alltid velger den beste løsningen innenfor brannmur.	Hendelsen blir vurdert som sannsynlig. Karakter = 3	Hendelsen blir vurdert som katastrofal. Karakter = 5
12	Dok.nr. 2.2. sier at trusselaktører leter etter sårbare servere, brannmurer, rutere og svitsjer. Disse blir utnyttet til å omgå tekniske sikringstiltak.	Informant B sier at ved implementering av Splunk kommer det utfordringer knyttet til den teknologiske forståelsen. Avhengige av et eksternt firma ved implementeringen av Splunk.	Hendelsen vurdert som sannsynlig. Karakter = 3	Hendelsen vurdert som kritisk. Karakter = 4

Norsk leverandør verdikjede

NR	Dokumentanalyse	Intervju	Sannsynlighet	Konsekvens

5	Dok.nr 2.2 sier at virksomheter i liten grad har kjennskap til konsekvenser av bortfall kraftleveranser, hvordan dette vil påvirke resten av verdikjeden.	Informant B sier at menneskelige feilhandlinger utgjør omlag 20-50% av årsaken til sikkerhetsbrudd.	Hendelsen vurderes som lite sannsynlig. Karakter = 2	Hendelsen vurderes som farlig. Karakter = 3
6	Dok.nr 2.2 sier at virksomheter i liten grad har kjennskap til konsekvenser av vesentlig ustabil tilgang i en kompleks verdikjede.	Informant B sier at man må ha kontroll på teknologien som er brukt, men i den verdikjede vil det være utfordrende å holde oversikt over alle mulige sårbarheter.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som lite farlig. Karakter = 2
7	Dok.nr. 2.3 sier at datanettverks-operasjoner utgjør en betydelig trussel for Norge, hvor rekruttering av innsidere gjør at man kan få tilgang til lukkede nettverk.	Informant B sier at det er en utfordring å påse hvor brukere skal få tilgang og ikke i brannmurer, og eventuelle åpne porter i ruter og svitsjer.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som katastrofal. Karakter = 5
8	Dok. 1.2 sier at ukryptert programvare eller maskinvare som blir implementert tilfører utilsiktede sårbarheter.	Informant B sier at jo lengre inn i nettverket man kommer jo vanskeligere blir det å kompromittere data, men den nye plattformen Splunk krever avansert teknologiske kunnskaper som kan utgjøre sårbarheter.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som kritisk. Karakter = 4
9	Dok.nr 2.6 viser til at av 572 deltakere fra undersøkelsen er det 39% som sier at mangel på sikkerhetsbevissthet hos ansatte var årsaken til sikkerhetsbrudd.	Informant F sier at man daglig opplever forsøk på digitale angrep, og jo flere systemer som blir sammenkoblet jo vanskeligere blir det med å detektere hvor sårbarheten ligger.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som kritisk. Karakter = 4
10	Dok.nr 2.6 sier at mangel på kompetanse for anvendt teknologi utgjør 20% av årsaken til at sikkerhetsbrudd oppstår.	Informant F sier at ny teknologi vil føre til mer risiko, og dersom man ikke forstår teknologien vil det utgjøre en stor risiko.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som lite farlig. Karakter = 2
11	Dok.nr 2.6 sier at 18% av 572 undersøkte hadde manglende oppdatering av utstyr eller konfigurasjon førte til sikkerhetsbrudd og 6% sier det skyldes problemer knyttet til outsourcingspartner.	Informant B sier at tap av måledata er kritisk og dersom man ikke har kontroll på måledataen så utgjør det en betydelig sårbarhet.	Hendelsen vurderes som lite sannsynlig. Karakter = 2	Hendelsen vurderes som katastrofal. Karakter = 5
12	Dok.nr 2.6 viser at årsaken til sikkerhetsbrudd i 20% av de 572 undersøkte at mangelfulle prosedyrer var årsaken. Videre sier rapporten at 28% av årsakene skjedde som følge av at eksisterende prosesser ikke ble fulgt.	Informant A sier at leverandører aldri er inne i nettverket for overvåkings-senteret, men at man ikke får testet teknologien fra leverandører.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som farlig. Karakter = 3

Transnasjonal leverandør verdikjede:

NR	Dokumentanalyse	Intervju	Sannsynlighet	Konsekvens
5	Dok.nr 2.6 viser at 28% av årsakene til sikkerhetsbrudd skjedde som følge av at eksisterende prosesser ikke ble fulgt.	Informant D sier at man ikke har kontroll på alle leverandørene i hele verdikjeden, da der er for mange ledd.	Hendelsen vurderes som lite sannsynlig. Karakter = 2	Hendelsen vurderes til farlig. Karakter = 3
6	Dok.nr 2.6 sier 18% av 572 at manglende oppdatering av	Informant G sier at det er utfordringer med å få teknologi til å snakke sammen på tvers av sektorer,	Hendelsen vurderes som	Hendelsen vurderes som

	utstyr eller konfigurasjon førte til sikkerhetsbrudd.	hvor tilgjengeligheten eksterne og interne brukere ikke kan garanteres.	meget sannsynlig. Karakter = 4	farlig. Karakter = 3
7	Dok.nr 2.2 fremhever som en av tre risikofaktorer som påvirker nasjonal sikkerhet at økende avhengighet av digitale infrastrukturer og verdikjeder som er transnasjonale.	Informant F sier at de ikke har ressurser eller kompetanse til å ha løpende vurdering av leverandører, at man må stole på leverandøren.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som katastrofal. Karakter = 5
8	Dok. nr 2.4 sier at transnasjonale verdikjeder underligger ulike jurisdiksjon som begrenser muligheten til å kontrollere sikkerheten, noe som innebærer en betydelig risiko.	Informant A og G sier at nettverket er segregert inn til overvåkings-sentrene for å hindre uautorisert adgang. Informant A sier at den måten de kontrollerer leverandører på er prisgitt i avtalen.	Hendelsen vurderes som svært sannsynlig. Karakter = 4	Hendelsen vurderes som kritisk. Karakter = 4
9	Dok.nr 2.2 sier at mange norske virksomheter opplever digitale innbrudd og misbruk av infrastruktur. Dok.nr 2.6 sier at 13% av 1500 virksomheter har opplevd forsøk på datainnbrudd eller hacking, hvorav 5% faktisk har hatt datainnbrudd.	Informant F sier at mer tilgjengelighet til data fører til endring av informasjons-sikkerhet som må være med i alle ledd, noe som ikke skjer i dag. Folk kan ubevisst dele brukerrettigheter som utgjør en betydelig risiko for integriteten og konfidensialiteten til data.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som kritisk. Karakter = 4
10	Dok.nr 2.6 sier at 7% av de 1500 virksomhetene ble utsatt for tjenestenektangrep eller forsøk på det.	Informant C sier at man selv må stå til ansvar for å oppdage at skyleverandøren har oppdatert sitt system og gjøre følgende vurderinger for å tilpasse seg de nye endringene.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som farlig. Karakter = 3
11	Dok.nr 2.6 sier så mye som 55% av tilfellene ved sikkerhetsbrudd var menneskelige feil årsaken.	Flere informanter peker på at en innsider er meget sannsynlig.	Hendelsen vurderes som meget sannsynlig. Karakter = 4	Hendelsen vurderes som katastrofal. Karakter = 5
12	Dok.nr 2.6 sier at mangelfulle prosedyrer utgjorde 20% av årsaken til sikkerhetsbrudd, og 19% til nedprioritering av sikkerhetsarbeid.	Informant D sier at det forekommer brudd i prosedyrer i form av at ansatte ved en feil setter andre på kopifeltet som ikke skulle vært der og dermed lekker sensitiv informasjon til uautorisert brukere.	Hendelsen vurderes som sannsynlig. Karakter = 3	Hendelsen vurderes som kritisk. Karakter = 5

9.5 VEDLEGG 5: BEGREPSAVKLARING FOR MÅLEINSTRUMENT FOR NVE

Global Navigation Satellite System (GNSS) er en fellesbetegnelser på satellittbaserte systemer for navigasjon, posisjonering og tidsangivelse, det er også kjent som satellittnavigasjonssystemer. NVE benytter GNSS-antenner, og ett eller flere faste referansepunkt for støykorreksjon i den kontinuerlige overvåkningen av ustabile fjellparti. Måling ved hjelp av faste referansepunkt blir kalt differensiell GNSS (sGNSS) og skal gi en målepresisjon helt ned til millimeteren. Ut ifra behovet til det risikoutsatte fjellpartiet kartlegges det behovet for antall GNSS antenner. Måledata blir prosessert ved å måle posisjonen horisontalt og vertikalt i 3D over 15 minutter, 4 timer og 12 timer. Fra resultatet kan en kartlegge bevegelser i de ustabile områdene ved at posisjonen til de faste referansepunktene forflytter seg [61].

Bakkebasert radarmåling/GB-InSAR (Interferometrisk syntetisk apertur-radar fra bakken) fungerer ved å analysere reflektert signal mellom to radarbilder som er tatt på forskjellige tidspunkt av det samme området. Dette gir en indikasjon på om avstanden har endret seg mellom de to tidspunktene og kan si om det er bevegelser i de ustabile fjellpartiene. Denne metoden blir brukt for å kunne kartlegge nye områder som potensielt kan være høyrisikoobjekter. Målingene blir utført i samarbeid med det italienske selskapet Ellegi_srl som bistår til drift av flere radarer ved bruk av et LiSALab system. LiSALab er et fjernovervåkningssystem som måler bevegelser i bakken ved hjelp av radarmåling [27]. Resultatet av denne type radarmåling gir sanntidsobservasjoner. SVF har i tillegg utviklet en transportabel radar i form av en tilhenger som kan fraktes hurtig til ønsket sted for sanntidsobservasjoner [28].

Satellittbasert radarmåling/SB-InSAR (Interferometrisk syntetisk aperture rader) brukes i likhet med GB-InSAR for å kartlegge avstandsendring ved å analysere to radarbilder som blir reflektert på forskjellige tidspunkt. Satellittene er plassert i en 800 kilometers høyde i atmosfæren og måler forflytningen på jordoverflaten. Historiske radarsatellittbilder kan også gi en indikasjon på tidligere bevegelser som kan være nyttige i predikasjoner om hvordan bevegelsene oppfører seg [16].

Laser er et måleinstrument som blir brukt til å måle lange avstander og fungerer ved at en fastmontert laser sender ut laserstråler til en reflektorplate for å måle avstanden. Laserstrålen beveger seg med lysets hastighet og hastigheten er den avgjørende faktoren for å måle avstanden. Måten en analyserer avstanden på er ved å se på tiden laserstrålen bruker over til reflektorplaten, tidsdifferansen viser dersom det skulle være bevegelse ved at den bruker mer eller mindre tid til å treffe reflektorplaten [62].

Totalstasjon består av en laser som måler 3D-bevegelser ved hjelp av horisontale og vertikale vinkler, samt avstander til flere referanseprismer som står på utvalgte steder for området som skal overvåkes. Totalstasjonens innmålinger gir en nøyaktighet helt ned til noen få millimeter, noe som gir svært detaljerte avstandsmålinger. Stedet til totalstasjon er utvalgt med hjelp av GNSS-målinger til fri sikt ut til prismene, samt for å forsikre at totalstasjonen står på et stabilt underlag [63].

Ekstensometer er en fellesbetegnelse for mekaniske avstandsmåle-instrumenter. Bruksområdet til måleinstrumentene er sprekkeåpninger og måler sprekkene over tid. For

fjellskredovervåkningen brukes det tre typer ekstensometer; ekstensometer, crackmeter og draw-wire. Ekstensometer måler avstander på en meter, og instrumentet har selv en lengde på to til tre meter. Crackmeters måleområde er 10 cm, med en egen lengde på 30 cm. Draw-wire har mulighet til å måle opp til 15 meter med samme lengde på instrumentet [17].

Tiltmeter er et elektronisk vater som brukes til å måle rotasjoner i borehull, utvelting av blokker og hellingsgrad. I tillegg kan tiltmeter brukes til å forhindre at andre installasjoner som totalstasjon roterer [18].

Værstasjon blir brukt til å måle luft og fjelltemperatur, vindstyrke og retning, nedbør og snødybde. For fjellparti med kontinuerlig overvåking er det en tilhørende værstasjon plassert ute i feltet. Måledata fra værstasjonen kan brukes til å sammenligne data fra andre måledata for å si noe om klimaendringer gir utslag på bevegelser i fjellet [64].

Borehullinstrument er utstyr med lange strenger bestående av ulike instrumenter som kommer fra det italienske selskapet CSG. Instrumentene kan være tiltmeter, piezometer, temperatursensorer og puter. Ved bruk av disse instrumentene kan en kartlegge bevegelsesretningen og vanntrykket med temperatur til borehullet, og puter brukes for å kunne gi en enda mer korrekt måleverdi på vanntrykket [65].

Seismiske instrumenter består av seismometer som er et veldig følsomt instrument som blir brukt til å måle rystelser i bakken, og geofoner som er langt mindre følsomme. Følsomheten til seismometer instrumentet måler trykkbølger i tre ulike retninger og gir en nøyaktighet på mikro- og nanometernivå. Geofoner måler også lokale trykkbølger i tre ulike retninger [66].

Strekkstag er et måleinstrument for å detektere bevegelser ved å plassere den ene enden av strekkstagen på et fast fjell og den andre delen på det ustabile fjellet. Strekkstagen består av to stålrør som ligger i hverandre med sensorer som detektere dersom strekkstaget skulle bevege seg i en av retningene [67].

Webkamera av typen overvåkningskamera er den mest anvendte overvåkingsteknologien hvor en har mulighet til å rotere kameraet 360 grader med zoomfunksjoner. Denne type kamera er brukt som overvåkning av alle risikoobjekter som har kontinuerlig overvåkning. Kameraene gir mulighet til å utforske skredområder, vurdere om værholdene er gode nok for å fly ut i feltet og sammenligne værdata fra annen måledata [68].