Universitetet i Stavanger

DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Master i teknologi - Risikostyring	Vårsemesteret, 2014 Åpen / ~~Konfidensiell~~
Forfatter: Truls Gundegjerde	Truls Gundegjerd ..... (Signatur forfatter)

Fagansvarlig:
Eirik Bjorheim Abrahamsen

Veileder:
Eirik Bjorheim Abrahamsen

Tittel på masteroppgaven:
Risikoanalyse av IT-systemer

Engelsk tittel:
Risk analysis of IT systems

Studiepoeng:
30

Emneord: - Risikoanalyse - Grovanalyse - IT-risiko - Usikkerhet - Risikodefinisjon	Sidetall: 68 Stavanger, 12.06.2014

Forord

Denne oppgaven markerer avslutningen på mitt masterstudie innen risikostyring ved Universitetet i Stavanger. Jeg ønsker med dette å benytte anledningen til å takke alle som har vært til hjelp under skrivingen av oppgaven.

Spesielt vil jeg takke Mari Lillejord for mange gode kommentarer og innspill.

I tillegg vil jeg rette en stor takk til min veileder Eirik Bjorheim Abrahamsen som har vært med gjennom hele prosessen. Takk for god støtte og veiledning, din kunnskap og dine kommentarer settes stor pris på.

Sammendrag

Oppgaven tar for seg noen etablerte risikoanalyser og veiledninger for å studere hvordan en i dag analyserer IT-risiko. Det vil innledningsvis bli gitt en gjennomgang av disse rapportene som da vil være grunnlaget for videre diskusjon. Et aspekt som det viser seg har fått lite plass i disse rapportene er usikkerhet. Dette vil være usikkerhet knyttet til konsekvens og tilhørende sannsynlighet.

Risiko forbundet med IT-systemer har i de siste årene økt med høy takt. I dagens samfunn består veldig mange tjenester av store og komplekse systemer alt i fra middagsplanleggings-app for smarttelefoner, til signering og godkjenning av juridiske dokumenter ved hjelp av BankID. Alle disse systemene medbringer risikoer som bør analyseres.

Gjennom et eksempel som omhandler *Tingenes internett* og videre *smart hus* vil en legge frem forslag og argumenter for at det vil være hensiktsmessig å endre på hvordan risiko blir definert innenfor IT-bransjen. Det vil være fordelaktig å gå fra en definisjon som tar for seg uønskede hendelser med konsekvenser og tilhørende sannsynligheter til et syn hvor en også inkorporerer usikkerhet. Det vil si en definisjon på risiko som en todimensjonal kombinasjon av hendelsen A og konsekvensen av denne, C, på den ene siden og de tilhørende usikkerhetene på den andre siden, (Aven, 2008). Eksempelet viser at en ved å endre definisjonen på risiko kan få en bedre risikoanalyse som gir mer nyttig informasjon, som igjen gir en bedre beslutningsgrunnlag.

Innhold

1 Innledning

Risikoanalyser av IT-systemer begynner å bli mer utbredt enn det lenge har vært. Tidligere har både privatpersoner og bedrifter fått tak i ny program- og fastvare og satt denne i drift umiddelbart uten å tenke noe mer over risikoen ved å implementere et nytt system. I nyere tid er denne trenden i midlertid i ferd med å snu, det blir nå oftere gjennomført risikoanalyser av IT-systemer som skal tas i bruk hos bedrifter og privatpersoner er i ferd med å innse at det å ha dusinvis med internettilkoblede enheter i hjemmet kan utgjøre en risiko. Årsaken til at IT-risiko nå har blitt mer utbredt hos bedrifter kan være flere, der i blant nye lover og regelverk som krever risikoanalyser samt den økende sofistikerte cyberkriminaliteten.

Utviklingen av internett som vi kjenner det er i ferd med å skifte toneart, *tingenes internett* er for fullt i anmarsj. I begrepet tingenes internett tar en for seg den nye digitale hverdagen hvor objekter har fått internettilgang og er i stand til å kommunisere med hverandre uten hjelp fra bruker. Antall internettilkoblete enheter øker i et raskt tempo, denne økningen fører med seg store muligheter både for privatpersoner og bedrifter så vel som for samfunn og myndigheter. Ettersom flere og flere etter hvert får øynene opp for de uendelige mulighetene endringen av internettet medbringer, er det kanskje ikke like mange som tenker på risikoen denne endringen kommer med. Oppgaven vil ta for seg et gitt antall IT-risikoanalyser og gjennomgå hvordan risikoen her blir vurdert, videre vil det bli gjort et forsøk på å lage et rammeverk på hvordan IT-risiko best kan bli vurdert. Til dette vil et eksempel på analyse av IT-risiko knyttet til tingenes internett bli gitt.

Gjennom bruk av risikoanalyser får man en bedre oversikt over risikobildet som det analyserte risikoobjektet medbringer. Det finnes ferdigdefinerte analyser og brukerveiledninger som kan være til hjelp når et IT-system skal analyseres. Som nevnt vil noen av disse veiledningene og rapportene bli sett nærmere på i denne oppgaven, diskutert og sammenlignet for å identifisere likheter/ulikheter, styrker og svakheter. Et moment som ofte ikke får mye spalteplass i risikoanalyser av IT-system er usikkerhet. Risiko blir ofte presentert med sannsynligheter og forventningsverdier på hva som kan skje og om det vil skje. I denne forbindelse er det viktig å understreke er at alle typer usikkerhet i forhold til hva som kommer til å bli konsekvensene ikke reflekteres gjennom sannsynligheter (Aven, 2008). Oppgaven vil dermed legge vekt på å sammenligne rapporter og veiledninger fra industrien for å se hvordan disse fremstiller risiko, om usikkerhet blir nevnt i noen form og deretter forsøke å foreslå en mulig måte å kombinere IT-risikoanalyser med usikkerhet.

1.1 Bakgrunn

Med undertegnedes bakgrunn fra datateknikk i tillegg til risikostyring var det ønskelig å konstruere en tverrfaglig oppgave. Tingenes internett er i ferd med å få fotfeste rundt om i verden og det er noe vi kun har sett starten på, men som vil komme til å prege hverdagene for alle og enhver i fremtiden. Ved nye ting og muligheter kommer også risiko, IT-risiko har vært et tema som i den siste tiden har begynt å blomstre og som stadig flere aktører legger tid og penger ned i. Risikobildet rundt bruken av internettilkoblete enheter er i ferd med å øke ettersom det nå er mye å hente for kriminelle i forhold til hva de kunne få til for noen år tilbake. Ved å kombinere IT-risiko med risikobildet rundt tingenes internett får en mulighet til å se på metodikken rundt IT-risikoanalyser og en kan trekke inn usikkerhet.

1.2 Mål og bidrag

Målet med oppgaven er, ved å gjennomgå etablerte risikovurderinger og analyser, å komme frem til en form for retningslinjer for hvordan IT-risiko kan bli vurdert/analysert. Oppgaven tar for seg fire forskjellige analyser/vurderinger av risiko tilknyttet IT. En gjennomgang av disse skal kunne hjelpe til å legge grunnlaget for retningslinjene på hvordan en IT-risikoanalyse kan gjennomføres. For å belyse noen poeng, og for å synliggjøre analysemetoden, vil det bli gjort en risikovurdering av et delsystem av tingenes internett, nemlig *smarthus*. Her skal det nevnes at resultatet av denne analysen i seg selv ikke er det vesentlige, snarere hvordan analysen er bygget opp og hvilke elementer som blir tatt med. Som nevnt tidligere er usikkerhet noe som ofte ikke blir diskutert i risikoanalyser av IT-systemer, i oppgaven vil usikkerhet bli sett nærmere på og vil bli brukt i analysen av *smarthus*. Resultatet fra eksempelanalysen skal visualiseres ved hjelp av en risikomatrise.

1.3 Komposisjon

Kapittel 2 inneholder en gjennomgang av fire forskjellige risikovurderinger/analyser hentet fra næringslivet. Rapportene fra disse analysene vil bli lagt til grunn for videre diskusjon og tatt i betraktning når en samlet måte for risikostyring av IT-systemer presenteres. I kapittel 3 diskuteres forskjellige aspekter av de nevnte rapportene slik at en best mulig kan bruke kunnskap fra disse til å sette sammen hovedproduktet. I dette kapittelet introduseres og presenteres også usikkerhet. Kapittel 4 inneholder videre diskusjon og forslag, i form av et flytskjema, på hvordan en kan analysere IT-risiko hvor også usikkerhet er tatt med. I kapittel 5 brukes flytskjema som utgangspunkt for eksempelet med smarthus. Videre følger en avsluttende konklusjon og diskusjon.

2 Gjennomgang av utvalgte analyser og retningslinjer

I det følgende kapittelet vil et utvalg av risikoanalyser, risikovurderinger og risikoveiledninger bli gjennomgått. Hensikten med denne gjennomgangen er å vise hvordan IT-risiko blir analysert og vurdert hos forskjellige instanser/bedrifter. Analysene blir sammenlignet hvor svake og sterke sider vil bli diskutert. Rapportene skal bli brukt som utgangspunkt for å kunne gi generelle retningslinjer for hvordan å gjennomføre en risikoanalyse av et IT-system.

Rapportene som vil bli diskutert videre er følgende:

- *Risikovurdering av informasjonssystem* – Datatilsynet (Datatilsynet, 2002)
  Datatilsynets risikovurdering opptrer som en form for mal som ulike bedrifter kan benytte seg av, og er av den grunn valgt til å være en av referansene i denne oppgaven. Eksempelvis har difi – direktoratet for forvaltning og IKT brukt Datatilsynets veiledning i sin egen veiledning, se (Difi, 2010).
  Referansen blir videre i oppgaven kalt for referanse A.

- *Nasjonalt senter for samhandling og telemedisin – risikovurdering* (Henriksen & Skipenes, 2013)
  Denne veiledningen/rapporten er valgt for å vise hvordan IT-risiko blir vurdert i kommuner og for å se om dette blir gjort annerledes i helsesektoren enn i for eksempel malen fra Datatilsynet.
  Referansen blir videre kalt for referanse B.

- *ROS-analyse, Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT)* – Finanstilsynet (Finanstilsynet, 2012)
  Finanstilsynets ROS-analyse ble valgt fordi den er bygget opp på en annen måten enn hvordan andre mer «vanlige» analyser er byttet opp. I tillegg er det interessant å ta med en referanse som bringer frem IT-risiko innenfor finanssektoren som også opplever store økninger i angrep og tekniske utfordringer.
  Referansen blir videre kalt for referanse C.

- *Risk assessment for altering and monitoring of the statewide microwave network* – Department of Administration State Information Technology Services Division

(Department of Administration State Information Technology Services, 2011)

For å få et mer helhetlig utgangspunkt ble det valgt å ta med en risikovurdering som ikke hadde sitt opphav i Norge. Risikovurderingen av endring og overvåkning av mikrobølgenettverket i Montana gir dermed et litt annet utgangspunkt, som kan være greit å inkludere. I tillegg er nevnte rapport valgt til å bli tatt med fordi den er mer et ferdig produkt av en faktisk analyse. Noen av de andre er bygget mer opp som guidelines eller som en mal.

Referansen blir videre kalt for referanse D.

Etter gjennomgang av de valgte rapportene og veiledningene, samt kommentarer til disse, vil kapittel med videre diskusjon følge. Som nevnt tidligere er hensikten med denne gjennomgangen å vise hvordan analyser og vurderinger blir utført i dag, en ønsker å gi leseren et innblikk i hvordan en risikoanalyse eller en risikovurdering blir gjennomført hos forskjellige bedrifter i forskjellige sektorer, både i Norge og i utlandet.

2.1 Risikovurdering av informasjonssystem – Datatilsynet

Innholdet i de påfølgende avsnittene er hentet fra og inspirert av (Datatilsynet, 2002).

Datatilsynet har publisert en veiledning til hvordan de anbefaler større og mindre bedrifter til å gjennomføre en risikovurdering av et informasjonssystem. Datatilsynet gir uttrykk for at denne risikovurderingen kan brukes i forskjellige sektorer i samfunnet men legger ved at metoden beskrevet her i første omgang skal dekke kravet i personopplysningsforskriftens bestemmelse om risikovurdering, ettersom mange IT-systemer behandler personopplysninger. I forbindelse med personopplysningsforskriften og personvern vil en knytte tre aspekter sammen for å identifisere risiko, disse er *konfidensialitet, integritet* og *tilgjengelighet.*

Datatilsynet starter med å identifisere akseptabelt risikonivå, det vil si risikoakseptkriterier. Disse akseptkriteriene har en vesentlig rolle i risikostyring, da de er holdepunkter og er nødvendige å ha slik at dersom risikoen øker kan dette måles i forhold til kriteriene og dermed bestemme om risikoen er for høy og handle deretter. Videre legger Datatilsynet ved en del innspill til hvordan disse akseptkriteriene kan og skal være. Datatilsynet legger også ved noen tanker om planlegging og organisering, etterfulgt av kartlegging av verdier.

Videre blir uønskede hendelser identifisert. Her kommer igjen de tre aspektene inn i bildet, manglende konfidensialitet, tilgjengelighet eller integritet. Datatilsynet velger å si at disse verdiene kan grovt sett påvirkes av tre typer uønskede hendelser; *utlevering, utilgjengelighet* og *endring*. Disse hendelsene blir deretter videre detaljert ved å inkludere kompensering varighet og deteksjon. Dermed kan de tre uønskede hendelsene beskrives som følger;

Utlevering	**Kan tilbakeføres**
	Permanent
Utilgjengelighet	Avgrenset tidsrom
	Permanent
Endring	Sporbar og kan rettes
	Sporbar og permanent
	Ikke sporbar

Tabell 1 Klassifisering av uønskede hendelser hentet fra (Datatilsynet, 2002)

Ved identifisering av uønskede hendelser er det viktig at arbeidet konsentreres om hendelser som faktisk medfører en risiko. Antallet uønskede hendelser kan ofte bli veldig stort dersom man ikke begrenser arbeidet. Datatilsynet nevner her at utvelgelsen må ta utgangspunkt i det taps- eller skadepotensiale som tidligere er anslått når verdier og miljø ble kartlagt.

Etter identifisering av uønskede hendelser følger underkapittel om årsaker. Datatilsynet beskriver årsaksanalysen som en aktivitet for å besvare spørsmål som *hvordan* en uønsket hendelse har oppstått, ofte trekkes også *hvem* inn i dette spørsmålet. Spørsmålet om hvem kan grovt inndeles i «interne medarbeidere» eller «eksterne medarbeidere». Det legges vekt på å formidle at hendelser og årsaker skal beskrives hver for seg, et manglende skille vil kunne resultere i detaljerte beskrivelser som ser ut til å dekke en rekke hendelser men som egentlig viser seg å bare beskrive en hendelse med et antall mulige årsaker.

Ved å bruke analogien som Datatilsynet har brukt skal konsekvensvurderingen vurdere hvilke følger en uønsket hendelse kan få, den skal altså gi svar på spørsmål som *hva medfører*. Ofte blir konsekvenser uttrykt som økonomisk tap men det nevnes at også virksomhetens anseelse kan uttrykke konsekvens. Datatilsynet nevner i avsnittet om konsekvensvurdering at konsekvenser må angis kvalitativt som en beskrivelse om hva konsekvensen faktisk innebærer, i tillegg er det viktig for det videre arbeidet og for å få et risikobilde som resultat av vurderingen at konsekvensene også får en kvantitativ størrelse. Et eksempel på en kvantitativ beskrivelse av konsekvensene blir lagt frem av Datatilsynet og er på følgende form;

- *K=4 – katastrofal konsekvens*
- *K=3 – stor konsekvens*
- *K=2 – moderat konsekvens*
- *K=1 – liten konsekvens* (Datatilsynet, 2002)

Videre i retningslinjene beskriver Datatilsynet at de konsekvensklassene nevnt over kan tilpasses videre, i dette tilfellet til personvernkonsekvens. Hver av de fire klassene får da en beskrivelse over hva konsekvensklassen innebærer for personvern, eksempelvis bli K=4 oppdatert til å inneholde følgende;

- *K=4, hendelsen kan føre til tap av liv eller vedvarende helsetap, eller kan medføre betydelig og uopprettelig økonomisk tap, eller kan føre til alvorlig tap av anseelse eller integritet som påvirker liv, helse eller økonomi.* (Datatilsynet, 2002)

Når mulige konsekvenser er beskrevet må en vurdering av sannsynligheter på plass. Her legger Datatilsynet ved flere mulige metoder å utføre vurderingen på. Sannsynligheter skal også beskrives kvantitativt, som for konsekvensene. Den første og mest opplagte metoden som blir presentert er vanlig klassifisering etter hvor høy/lav sannsynlighet en hendelse har. Dette gjøres ved å etablere fire nivåer (S=4, S=3, S=2 og S=1) som beskriver sannsynlighetsgradene *svært høy, høy, moderat* og *lav*. Neste mulige metode som blir

presentert er en letthetsvurdering, her brukes de samme klassene S4-S1 men hver av klassene blir definert etter hvor lett hendelsene kan inntreffe. Her nevnes det hendelser, utforming av miljø og hvilke tekniske sikkerhetstiltak som er implementert og hvordan disse virker. Et eksempel på dette er;

- *S=4, sikkerhetstiltak er ikke etablert, eller kan omgås/brytes av egne medarbeidere og eksternt personell med små til normale resurser. Det er ikke nødvendig med kjennskap til tiltakene.* (Datatilsynet, 2002)

En tredje metode for sannsynlighetsvurdering er å ta utgangspunkt i motivasjon, her menes det at sannsynligheten beskrives i form av hvordan andre kan nyttiggjøre seg av informasjonen. Det blir nevnt at det ofte kan være vanskelig å identifisere motivet bak en hendelse og at det derfor er bedre å fokusere på innsatsen som må til for å forårsake hendelsen. Eksempelvis blir klassen S=4 definert som;

- *S=4, sikkerhetsbrudd kan skje ved uaktsomhet (ubevisst eller uten forsett) av egne medarbeidere eller utenforstående. Det er ikke nødvendig med spesielle kunnskaper om interne forhold.* (Datatilsynet, 2002)

For å presentere risikonivået bruker Datatilsynet en grafisk presentasjon i form av en risikomatrise. De definerer risiko som en kombinasjon av konsekvens av en hendelse og sannsynligheten for at denne inntreffer. I matrisen plasseres sannsynlighet og konsekvens som danner et bilde på risikonivået, hvor også akseptabelt risikonivå er markert (ikke-skravert område). Eksempel på risikomatrise:

Konsekvens → ↓Sannsynlighet	Liten	Moderat	Stor	Katastrofal
Lav				
Moderat				
Høy				
Svært høy				

Figur 1 Risikomatrise fra Datatilsynet, (Datatilsynet, 2002)

Når risikobildet er presentert er siste punkt å komme med anbefalt tiltak for identifiserte hendelser som har en risiko som er høyere enn akseptabelt nivå. Datatilsynet nevner at valg av sikkerhetstiltak ikke er en del av selve risikovurderingen, men at de resultater som vurderingen kommer med bør etterfølges av anbefalte tiltak. Tiltak som blir presentert kan bli delt inn etter om de skal være forebyggende eller skadebegrensende, tiltak blir dermed

klassifisert etter hva de er ment å gjøre mot/for hendelsen; unngås, avskrekkes, hindres, isoleres eller oppdages.

2.1.1 Kommentar til veiledningen fra Datatilsynet

I det foregående kapittelet ble Datatilsynets veiledning presentert. Veiledningen gjør et godt stykke arbeid med å legge frem måter hvordan en kan gjennomføre en risikovurdering. Hovedstrukturen har en relativt normal oppbygning med først kartlegging og fastsetting av akseptkriterier, fulgt av identifisering av uønskede hendelser og deretter årsaksanalyse, konsekvensvurdering og sannsynlighetsvurdering med beskrivelse av risikobildet til slutt. Disse punktene blir, som en vil se lengre nede også brukt av andre parter. Som en del av oppgaven har det tidligere blitt nevnt at et moment som ofte ikke får mye plass i risikovurderinger av IT-system er *usikkerhet*. I Datatilsynets veiledning gis det et lite avsnitt om usikkerhet;

> *«Risiko uttrykker en hypotese og må følgelig angis med en viss usikkerhet. Denne usikkerheten må angis – eller i det minste diskuteres – når resultatene fra risikovurderingen presenteres.»* (Datatilsynet, 2002)

Her legger forfatterne i det minste ved et utsnitt som nevner noe om usikkerhet. Ettersom dette er en veiledning for risikovurdering så kan det være vanskelig å si nøyaktig hvor mye arbeid Datatilsynet mener usikkerheten skal få. Ut i fra hvordan det er beskrevet over burde usikkerheten fått noe mer omtale i veiledningen fordi det ofte er usikkerhet knyttet til både hvilken hendelse som kan inntreffe og til konsekvensen av hendelsen. Måten Datatilsynet velger å presentere risikobildet på, i form av en risikomatrise, er en veldig vanlig metode og vil gå igjen hos flere av gjennomgangene som følger. Bruk av risikomatrise gir ofte et enkelt verktøy til å tegne et helhetlig bilde av risikoen som en står ovenfor.

2.2 Nasjonalt senter for samhandling og telemedisin – risikovurdering

Innholdet i det gjeldende delkapittel er i stor grad hentet fra (Henriksen & Skipenes, 2013)

NST har publisert en rapport som omhandler risikovurdering i forbindelse med elektronisk behandling av personopplysninger. Rapporten kan fungere som en mal for kommuner som skal vurdere risikoen av informasjonssikkerhet. Metodikken rundt risikovurderingen starter ved å introdusere viktig personell som bør være med på vurderingen. Her er det snakk om personer som har forskjellig kunnskap som er vesentlig for å få kunne opprette og utføre en risikovurdering.

Sikkerhetsaspektene som skal sees på i risikovurderingen er som følger; tilgjengelighet, konfidensialitet, kvalitet og integritet. Disse aspektene er definert i helseregisterloven paragraf 16. Videre følger kartlegging av trusler samt vurdering av risiko, denne prosessen tar utgangspunkt i NST til faktaark om risikovurdering (NST, Nasjonalt senter for samhandling og telemedisin, 2013)

For å kunne identifisere trusler og uønskede hendelser er det nødvendig for gruppen som skal vurdere risikoen å gå gjennom prosessen med meldingsutveksling slik at nødvendig personell har den nødvendige informasjonen. Ved kartlegging av trusler er det snakk om trusler som kan være en trussel mot aspektene nevnt over (tilgjengelighet, konfidensialitet, kvalitet og integritet). Arbeidet med trussel-identifisering blir foreslått til å følge en trusseltabell slik at informasjonen om de gitte truslene kan systematiseres umiddelbart. NST velger å bruke denne tabellen også til videre arbeid, det vil si at dette altså er et arbeidsredskap som trolig trenger en opprydning i løpet av arbeidet.

Eksempel på utdrag fra tabellen;

ID	Trussel / Uønsket hendelse	Årsak	Sannsynlighet	Konsekvens	Risiko	Kommentarer, f.eks. beskrivelse av implementerte tiltak.
t1	Meldingen kommer ikke frem til rett fagsystem/tjeneste i kommunen, de som skal ha meldingen får den ikke.	Avsender (fastlege eller HF) har valgt feil tjeneste /mottaker				

Tabell 2 Utdrag fra trusseltabellen, hentet fra (Henriksen & Skipenes, 2013)

Først identifiseres alle truslene, videre må hver trussel gis en sannsynlighet og en konsekvens. NST har lagt ved definisjoner som brukeren av veiledningen/analysen kan bruke, noen av disse kan en se bygger på Datatilsynets definisjoner (se kapittel 2.1). Sannsynlighet kan defineres som følger:

Sannsynlighet	**Frekvens**	**Sårbarhet** **Tiltak**	**Letthet/Vanskelighetsgrad** **Motivasjon**
Liten	Mindre enn 0,1 % av meldingene	Sikkerhetstiltak er etablert og fungerer etter hensikten	Må ha detaljkunnskap om systemet. Sikkerhetsbrudd kan bare skje med overlegg, bevisst handling.
Middels	Mellom 0,1 og 1 % av meldingene	Sikkerhetstiltak er etablert men fungerer ikke fullt etter hensikten	Sikkerhetsbrudd forutsetter noe kjennskap til systemet, og bevisste handlinger (ikke ved et uhell).
Stor	Mellom 1 og 10 % av meldingene	Sikkerhetstiltak er ikke fullt etablert eller de fungerer ikke etter hensikten	Sikkerhetsbrudd kan skje ved uaktsomhet eller feil bruk. Uten overlegg.
Svært stor	For minst 10 % av meldingene	Sikkerhetstiltak er ikke etablert	Sikkerhetsbrudd kan enkelt skje ved uaktsomhet eller feil bruk. Lett å gjøre feil. Uten overlegg.

Tabell 3 Definisjon av sannsynlighet, hentet fra (Henriksen & Skipenes, 2013)

Videre skal også alle trusler/hendelser gis en score for konsekvens. Her legger også NST ved en matrise med en rekke forskjellige definisjoner som kan bli brukt som hjelpemiddel ved fastsettelse av konsekvens.

Konsekvens	**Virksomheten**			**Pasienter**	
	Regelverk	**Økonomi**	**Anseelse**	**Økonomi**	**Anseelse/ rykte/integritet**
Svært alvorlig	Uforsvarlig helsehjelp. Alvorlig lovbrudd, fengselsstraff/ foretaksstraff (tap av rett til å utøve virksomhet)	Betydelig økonomisk tap. Uopprettelig	Alvorlig tap av anseelse, ødeleggende virkning for tillit og respekt	Betydelig økonomisk tap. Uopprettelig	Alvorlig tap av anseelse/ integritet. Får store konsekvenser for liv, helse eller økonomi
Alvorlig	Helsehjelp med util-strekkelig kvalitet Bøtestraff/ foretaksstraff (bot)	Økonomisk tap. Uopprettelig	Alvorlig tap av anseelse. Vedvarende virkning for tillit og respekt.	Økonomisk tap. Uopprettelig	Alvorlig tap av anseelse/ integritet. Påvirker liv, helse eller økonomi
Moderat	Hinder for utøvelse av effektiv helsehjelp. Mindre alvorlig lovbrudd/ forseelse. Advarsel/ pålegg (som første reaksjon).	Betydelig økonomisk tap. Kan gjen-opprettes	Tap av anseelse. Virkning for tillit og respekt	Betydelig økonomisk tap. Kan gjen-opprettes.	Tap av anseelse/ integritet. Kompromittering av krenkende opplysninger
Liten	Kortvarig hinder for utøvelse av effektiv helsehjelp. Ingen lovbrudd.	Økonomisk tap. Kan gjen-opprettes	Kortvarig tap av anseelse	Økonomisk tap. Kan gjen-opprettes	Tap av anseelse/ integritet. Kompromittering av lite følsomme opplysninger.
Ubetydelig	Irritasjonsmoment	Ingen økonomisk konsekvens	Ikke tap av anseelse	Ingen økonomisk konsekvens	Intet tap av brukerens anseelse/integritet

Tabell 4 Definisjon av konsekvens, hentet fra (Henriksen & Skipenes, 2013)

Når alle kolonnene i trusseltabellen er utfylt skal de forskjellige truslene plasseres i risikomatrisen. NST har valgt å definere risiko som kombinasjonen av trusselens sannsynlighet og konsekvens, dermed blir risikomatrisen som NST bruker til å beregne risikonivået som følger:

Konsekvens: **Sannsynlighet:**	**Ubetydelig**	**Liten**	**Moderat**	**Alvorlig**	**Svært alvorlig**
Liten	Lav	Lav	Lav	Middels	Middels
Middels	Lav	Lav	Middels	Middels	Høy
Stor	Lav	Middels	Middels	Høy	Høy
Svært stor	Lav	Middels	Høy	Høy	Høy

Figur 2 Risikomatrise, (Henriksen & Skipenes, 2013)

Til slutt må alle trusler eller hendelsene evalueres, trusler med høy risiko blir av NST ansett som uakseptable og trusler med nivå middels krever en individuell vurdering. I tillegg skal tiltak føres inn i trusseltabellen.

2.2.1 Kommentar til NST sin risikovurderingsmodell

Risikovurderingen fra NST er bygget opp noenlunde likt Datatilsynets rapport, en skal i midlertid notere at NST sin veiledning gir uttrykk for å ikke romme et like stort omfang som veiledningen fra Datatilsynet. En skal se opp for bruken av ferdigdefinerte trusseltabeller (dette blir diskutert videre under diskusjonskapittelet). Veiledningen gir i tillegg uttrykk for å være noe enkel. Usikkerhet blir ikke nevnt i veiledningen.

2.3 ROS-analyse, Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT) – Finanstilsynet

Innholdet i gjeldende delkapittel er hentet fra (Finanstilsynet, 2012).

Finanstilsynet har publisert en risiko- og sårbarhetsanalyse av finansforetakenes bruk av informasjonsteknologi, denne analysen vil i det følgende bli gjennomgått og senere brukt i diskusjon. Målet med analysen er å gi et bilde av risikoutviklingen i finanssektorens bruk av IKT og betalingstjenester slik at sektoren kan ligge i forkant av den økende elektroniske kriminaliteten. Rapporten fra analysen starter med å gjennomgå og beskrive trender innenfor IKT som kan ha betydning for risikohåndteringen i Norge. Finanstilsynet presenterer en rekke trekk og trender som har betydning for risikohåndteringen etterfulgt av en del rapporterte hendelser fra året som har gått.

Når funn og observasjoner er presentert følger neste kapittel om identifiserte risikoområder. Her gir Finanstilsynet uttrykk for hvilke områder de mener utgjør en risiko. Hovedområdene som blir publisert som risikoområder er *styring og kontroll, angrep på nettbaserte løsninger, kontinuitets- og katastrofeløsninger, risiko ved gamle og komplekse systemer* og *tilgang til betalingstjenester*. Videre presenteres det kort informasjon om Finanstilsynets videre oppfølging, her blir det nevnt ulike områder som vil bli sett videre på, uten at dette utdypes noe videre.

2.3.1 Kommentar til ROS-analyse fra Finanstilsynet

Oppbygningen av ROS-rapporten fra Finanstilsynet viker noe fra de foregående risikovurderingene som er presentert. Rapporten legger stor vekt på å kvalitativt beskrive både rapporterte hendelser, generelt om hvordan situasjonen med betalingsløsninger er og videre hvilke områder som Finanstilsynet mener er risikoområder. Det legges lite arbeid ned i å gjøre rapporten til et oversiktlig bilde over risikoer og sårbarheter, det er for eksempel ikke gitt noe informasjon om prioriteringer i forbindelse med hverken de identifiserte risikoområdene eller Finanstilsynets punkter for videre oppfølging. For å ha gjort rapporten bedre burde kanskje analysen fulgt en noe mer standardisert metodikk, som for eksempel veiledningen fra Datatilsynet. På denne måten kunne en raskere fått et overblikk over viktige risikoområder og uønskede hendelser. Ettersom dette er en rapport som i stor grad presenterer risikobildet «*slik det var*» i året som har gått finnes det historisk data som kunne vært til hjelp ved fastsetting av sannsynligheter for uønskede hendelser. Videre burde Finanstilsynet, som den foregående, også ha nevnt usikkerhet.

2.4 Risk assessment for altering and monitoring of the statewide microwave network

Montana State Information Technology Service Division har utført en risikovurdering av *endring og overvåkning av mikrobølgenettverket i Montana*, USA. Mikrobølgenettverket brukes av offentlig redningspersonell. Systemet opererer i smalbåndsområdet i VHF-frekvensområdet og bruker en beskyttet høykapasitets digital mikrobølgeryggrad for tale- og datatrafikk. Informasjonen i gjeldende kapittel er i stor grad hentet fra rapporten som ble publisert i forbindelse med risikovurderingen (Division of Administration, 2011)

Risiko blir definert som en funksjon av at sannsynligheten for en gitt fare-kilde sin evne til å utøve/utnytte en potensiell sårbarhet og den resulterende effekten på organisasjonen.

Risikovurderingsprosessen blir her definert som en ni-stegs prosess, disse stegene vil nå bli gjennomgått. Det første steget er, som for de tidligere nevnte metodene, å karakterisere systemet slik at det går klart frem hva som skal vurderes/analyseres. I dette tilfellet blir systemet lagt frem og det blir presentert hvordan systemet virker, hvem som kan administrere det og hvordan dette skal gjøres. Når systemet er presentert er neste steg å indentifisere potensielle farer. Her skilles det mellom fire forskjellige kategorier; naturskapte, menneskeskapte, miljø og systemdesign. Videre etter definering av disse hovedkategoriene lages det en matrise for hver kategori hvor hendelser og farer blir notert, her blir også motivasjon notert.

Punkt tre er identifisering av sårbarheter i systemet. Her brukes matrisene som ble laget i forrige punkt slik at potensielle sårbarheter kan kobles til respektiv farekilde. Potensielle sårbarheter blir funnet ved hjelp av nasjonale standarder. Videre, som punkt 4, følger kontrollanalyse. Dette punktet består i å analysere kontrollfunksjoner som allerede er planlagt for implementering for å minimere eller eliminere sannsynligheten for at en fare/hendelse resulterer i en hendelse grunnet sårbarhet i systemet. Måten kontrollanalysen blir gjennomført på er å kategorisere disse kontrollfunksjonene, eller barrierene, i to hovedkategorier; teknisk og ikke-tekniske kontrollfunksjoner. Eksempel på teknisk kontrollfunksjon kan være kryptering mens eksempel på ikke-teknisk kontrollfunksjon vil være prosedyrer eller rutiner for å bruke utstyret.

Nå som trusler og sårbarheter er identifisert kan sannsynligheten for at dette skjer bli adressert. Her bruker forfatterne av analysen ordet *likelihood* som et kvalitativt estimat på om et angrep mislykkes eller lykkes og eventuelt til hvilken grad angrepet lykkes. Utførende

noterer at denne metoden ikke presist reflekterer sannsynligheten for et suksessfullt angrep men velger å ta med dette kvalitative estimatet ettersom det kan hjelpe når en skal prioritere risikoer og ved evaluering av hvor effektive potensielle barrierer er. Videre blir tre likelihood-leveler definert; høy, medium og lav. Kategorien høy blir definert som at farekilden har høy motivasjon, den nødvendige kompetansen og barrierer (eller controls) som er implementert for å hindre at en sårbarhet blir utnyttet er lite effektive. Medium blir definert slik at farekilden er motivert og har ekspertise/kunnskapen som trengs, barrierene kan hindre eller forsinke utnyttelse av en sårbarhet. Den siste kategorien, lav, blir definert slik at farekilden mangler motivasjon og eventuelt også den nødvendige kunnskapen. Barrierene som er satt hindrer fullstendig eller sterkt vanskeliggjør at sårbarheten blir utnyttet. Likelihood-level blir så kombinert med sårbarhet i en matrise, slik at hver identifisert sårbarhet får en likelihood-level høy, medium eller lav.

Videre i analysen blir virkninger analysert, her kombineres sårbarheter med virkninger og virkningens størrelsesorden, dette blir presentert i en matrise. Virkninger blir definert som konsekvensen dersom systemet står ovenfor en «worst-case scenario». Som punkt 7 i analysen blir risikoen presentert. Risikoen kombinerer likelihooden av at en risiko oppstår med virkningene/konsekvensene denne får. Risikoen blir definert ved hjelp av følgende matrise som gir et tall på likelihood og virkning/konsekvens.

Threat Likelihood	**Impact**		
	Low (10)	Medium (50)	High (100)
High (1.0)	Low 10 X 1.0 = 10	Medium 50 X 1.0 = 50	High 100 X 1.0 = 100
Medium (0.5)	Low 10 X 0.5 = 5	Medium 50 X 0.5 = 25	Medium 100 X 0.5 = 50
Low (0.1)	Low 10 X 0.1 = 1	Low 50 X 0.1 = 5	Low 100 X 0.1 = 10

Figur 3 Likelihood/Threat-definisjon hentet fra (Department of Administration State Information Technology Services, 2011)

For nå å få en matrise for risikonivået for de definerte sårbarhetene kombinerer man informasjon som tidligere er lagt frem, matrisen for sannsynligheten/likelihood til definerte sårbarheter samt matrisen for med størrelsesordenen til konsekvensene/virkningene. Ved å kombinere dette i en matrise ender man opp med en risikoscore på mellom 1 og 100 for hver av de definerte sårbarhetene. Risikoen for hver sårbarhet kan deretter plasseres i risikoklassene *høy* (51-100), *medium* (11-50) og *lav* (1-10).

Når alle hendelsene/sårbarhetene har fått en risikoscore tas de som er i klassene medium og høy videre for håndtering og anbefaling i punkt 8. Håndtering av risiko blir delt inn i fem kategorier; *unngå*, *forhindring av tap* (ofte ved å redusere frekvensen eller sannsynligheten for tap), *reduksjon av tap* (reduserer kosten eller omfanget av et eventuelt tap), *dele/overføre kontraktsrisiko* (legger det finansielle ansvaret over på tredjepart) og *segregering av tap* (ved å gjøre en eller begge av følgende metoder; separering og duplisering). Videre blir det opprettet en tabell som kombinerer det foregående, en matrise som da inneholder sårbarhet, kontrollmetode (teknisk, ikke-teknisk), håndteringskategori og håndteringsanbefaling.

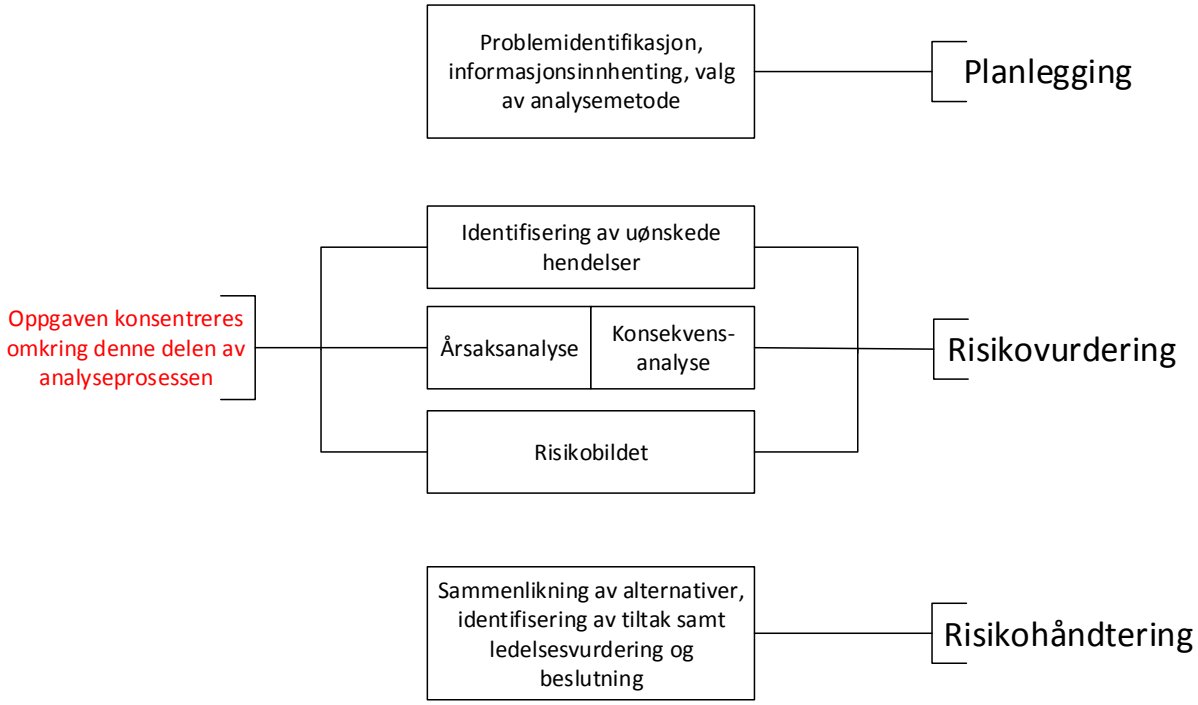
2.4.1 Kommentar

Risikovurderingen som beskrevet over har til en viss grad samme oppbygning som de foregående selv om vurderingen her blir delt opp i noen flere steg. Ved å ta med de ekstra stegene i prosessen gjør forfatterne det enklere for leseren av rapporten å trekke ut de viktige dataene. Videre ser en at bruken av matriser er stor i nevnte rapport, dette hjelper også på for å få et oversiktlig bilde av rapporten. Det skal likevel nevnes at en ikke har en like god matrise på det samlede risikobildet som en har i for eksempel referanse A og B. Usikkerhet blir ikke tatt med i risikovurderingen.

3 Diskusjon

Referansene som er presentert i forrige kapittel utgjør utgangspunktet for videre diskusjon. Hensikten med diskusjonen er å sammenlikne ulike aspekter fra de fire rapportene med hverandre, og senere å komme frem med et forslag/retningslinjer til hvordan å gjennomføre en risikoanalyse/risikovurdering av et IT-system.

Det skal nevnes at det i oppgaven legges vekt på *risikovurderingen*, det vil si den midterste delen av en risikoanalyseprosess. En risikoanalyseprosess er bygget opp av *planlegging*, *risikovurdering* og til slutt *risikohåndtering*.



Figur 4 Risikoanalyseprosess basert på (Aven, 2008)

Selv om en i oppgaven har valgt å legge vekt på risikovurderingsdelen er det ikke slik at de to andre delene av risikoanalyseprosessen ikke er viktige, snarere tvert imot. Planlegging av en analyse legger grunnlaget for hele analysen og dersom en ikke legger mye vekt på planlegging vil en kanskje oppleve at utfallet av analysen ikke er like bra som det kunne ha vært. Om utfallet av en risikoanalyse har blitt dårlig har det ofte blitt nevnt av analysegruppen at de feilene som ble begått, eller oversett, var grunnet snevert arbeid i planleggingsfasen. Dermed risikerer en at utfallet av analysen blir dårlig som videre medfører at beslutningsstøtten blir dårlig grunnet mangelfullt arbeid i planleggingsfasen. Det blir sagt at en mulig tommelfingerregel som kan benyttes her er at 1/3 av tiden skal gå med til planlegging av analysen, 1/3 til selve analysen og den siste tredjedelen til håndtering av

risiko, se (Aven, 2008). Som vist i figuren over så består planleggingsfasen av identifisering av kontekst, informasjonsinnhenting og valg av analyse. Inne i denne prosessen ligger også planlegging av ressurser og tid. Dermed er alt som gjøres i planleggingsfasen en veldig viktig del av risikoanalyseprosessen og det bør bli lagt mye arbeid ned i denne delen. Dersom en for eksempel går løs på risikovurderingen uten å ha lagt en plan over ressurser som trengs for å utføre analysen, kan en møte på problemer underveis som kan skape både forsinkelser og uante utgifter. Ta eksempelvis en analyse som blir utført for å vurdere oppgradering av kjøletårnet i et serverrom, midtveis i analysen viser det seg at analysegruppen trenger en full analyse av strømnettet i rommet for å kunne vurdere de forskjellige alternativene. Dermed måtte ekstern ekspertise ha blitt tilkalt for dette som igjen hadde medført forsinkelser og økte kostnader. Selvsagt kan en ikke alltid planlegge og ta høyde for alt men å legge arbeid ned i planleggingen vil som regel gi god avkastning.

Tilsvarende har risikohåndteringen også en viktig rolle å spille i en risikoanalyse, hva skal en gjøre med resultatet av analysen? Inn under delen av analysen som tar for seg risikohåndtering dekkes implementasjon av verktøy for å endre på risikoen som da inkluderer verktøy for å unngå, redusere, tolerere og dele risiko, (Aven, 2008). Ofte vil risikohåndteringen handle om valg av alternative løsninger basert på utfallet av risikoanalysen, dette kan som nevnt være valget mellom ventil A og B til bruk i et rørsystem eller det kan være valget av kjøleløsning for et serverrom.

3.1 Sammenlikning

De fire startreferansene A, B, C og D ble valgt ut for å gi et overblikk over hvordan IT-risiko blir analysert og vurdert. Den videre sammenlikningen og diskusjonen er bygget opp av de ulike elementene som er med i risikovurderingen, hvert element blir sammenliknet og diskutert. Først følger en drøfting av definisjonen på risiko etterfulgt av noen ord om struktur og komposisjon. Videre følger hovedpunktene i risikovurderingen som er identifisering av uønskede hendelser, årsaksanalyse, konsekvensanalyse og sannsynlighetstildeling etterfulgt av et avsnitt fokusert rundt usikkerhet og hvorfor dette er viktig å ta med. Til slutt trekkes visualisering inn i diskusjonen.

3.1.1 Definisjon

Det finnes mange ulike definisjoner på risiko og hva risiko er, noen mer intuitive enn andre. Eksempelvis defineres risiko av flere instanser som «*produktet av sannsynligheten for at en hendelse oppstår og konsekvensene av hendelsen*» det vil si sannsynlighet*konsekvens, se (Eilertsen, 2012), referanse A (Datatilsynet, 2002) og (Justis- og Beredskapsdepartementet, u.å.). En slik definisjon er relativt vanlig da den tar med både sannsynligheten for at en hendelse skal oppstå og konsekvensene denne hendelsen kan medføre. Det er i midlertid en dimensjon som denne definisjonen ikke legger vekt på, usikkerhet. Som nevnt er det av undertegnedes mening at usikkerhet er et moment som ofte får for lite plass i IT-risikoanalyser. Når en ser definisjoner som nevnt over kan en kanskje tenke at det ikke er rart, da selve definisjonen av risiko ikke nevner usikkerhet. Referanserapportene (A, B og D) tar alle i bruk sannsynlighet multiplisert med konsekvens når risiko skal defineres. I stedet for å kun se på de nevnte dimensjoner, sannsynlighet og konsekvens, er det viktig å ta med usikkerhet når risiko defineres. Dersom usikkerhet tas med i definisjonen kan en se på risiko slik som Petroleumstilsynet definerer risiko, nemlig som:

> *«Kombinasjonen av fremtidige hendelser og konsekvenser av disse, og tilhørende usikkerhet»*, se (Petroleumstilsynet, u.å.).

Av denne definisjonen ser en at usikkerhet knyttet både til den fremtidige hendelsen og konsekvensen av denne tas med. En liknende definisjon kan finnes i (Aven, 2008), som lyder som følger:

> *«Risiko er en to-dimensjonal kombinasjon av (i) hendelse A og de konsekvenser denne hendelsen medfører C, og (ii) den tilhørende usikkerheten U (om hva som vil bli resultatet)»*, se (Aven, 2008) .

Begge de to sistnevnte definisjonene tar altså med usikkerhet, hvorfor er det da slik at usikkerhet har fått så lite plass i de gjennomgåtte vurderingene og analysene? Er ikke usikkerhet et moment verdt å tenke på når det er snakk om IT-risiko? Som tidligere nevnte så var det kun referanse A, Datatilsynet, som nevnte usikkerhet med to korte setninger. Det er av undertegnedes oppfatning og mening at usikkerhet også burde få oppmerksomhet i forbindelse med risiko i IT-systemer.

Noe av årsaken til at usikkerhet ikke har sin plass i risikovurdering av IT-system kan kanskje være at IT-systemer tidligere var mer avgrenset, ofte ikke koblet til internett og med begrenset brukermasse. Det var kanskje lettere å identifisere mulige hendelser og fastsette sannsynlighet og konsekvens for disse. Nå i nyere tid er derimot systemene veldig komplekse og de aller fleste koblet til internett. Bare det faktum at et IT-system er tilkoblet internett øker risikoen (og usikkerheten) betraktelig. Cyberkriminalitet og angrep øker i et voldsomt tempo ettersom flere og flere tjenester bli nettbaserte, dette kan sees i rapporten fra Finanstilsynet (referanse C). Både ny teknologi og nye tjenester medbringer usikkerhet som må håndteres. Usikkerhet blir introdusert og diskutert videre i kapittel 3.1.7 og har i tillegg blitt valgt til å tas med i den generelle guidelinen som en til slutt skal ende opp med.

For å adressere usikkerheten i forbindelse med IT-risiko har definisjonen som inkluderer usikkerhet blitt valgt til å ta med i retningslinjene.

3.1.2 Struktur/komposisjon

Hvordan en risikoanalyse er bygget opp og hvilke elementer som blir tatt med er et viktig punkt. Referanserapportene har til dels lik oppbygging, sett bort i fra referanse C. Disse er bygget opp av en del som setter konteksten, definerer systemet og metodikk samt akseptabelt risikonivå, etterfulgt av identifisering av uønskede hendelser, årsaker til disse samt konsekvensen av disse. Videre følger fastsettelse av sannsynlighet for hver av de uønskede hendelsene og til slutt presentasjon av risikonivået, ofte i form av en risikomatrise.

Å ha en baktanke på hvordan analysen skal utføres og i hvilken rekkefølge de ulike delene av analysen skal få er viktig. Det er for eksempel viktig å ha klart definert hvordan systemet er bygget opp og hvilke deler som skal analyseres før en går i gang med identifisering av uønskede hendelser. Samtidig må uønskede hendelser identifiseres ferdig før disse kan bli håndtert videre, som nevnt kan en ikke håndtere det som ikke er kjent eller identifisert. Dette viser viktigheten av planleggingsfasen som kommentert i starten på kapittel 3, en kan spare seg for mye ekstraarbeid og feil ved å legge mye arbeid ned i planleggingsfasen.

Videre er det viktig å ha en struktur på analysen som gjenspeiler orden og kontroll slik at analysen kan brukes av annet personell enn bare analysegruppen som har utført arbeidet. I tillegg mener undertegnede at en skikkelig presentasjon av resultatet av analysen er viktig, ikke bare for at det skal se bra ut men for at beslutningstakere skal være fullstendig klar over hva som faktisk er utfallet av analysen. Samtidig er det viktig å notere seg at en fin visualisering av en dårlig utført analyse ikke automatisk gjør resultatet bra. Det samme gjelder motsatt vei, ved en utmerket analyse må resultatene presenteres skikkelig slik at de faktisk blir med i beslutningsgrunnlaget og ikke blir gjemt bort i mye tekst.

Referanse C er som tidligere nevnt bygget opp av rapporterte hendelser, denne bruken av rapporterte hendelser kan også være til nytte andre plasser. Ved gjennomførelse av en risikovurdering kan det være nyttig å innledningsvis ha oppsummert de største rapporterte hendelsene som er relatert til analyseobjektet. Dersom dette blir gjort vil en få kommunisert ut til alle i analysegruppen at dette er noe en må ha i baktankene, i tillegg vil det hjelpe til å starte tankegangen når uønskede hendelser skal identifiseres.

Når det gjelder oppbyggingen av analysen og hvordan den skal utføres er det en ting som kan nevnes; i referanse A blir det sagt at det er viktig å ha med all nødvendig personell til utførelsen av analysen i tillegg skrives det at en utenforstående skal hentes inn for å kvalitetssikre arbeidet. Dette trenger ikke alltid være en innleid ressurs eller konsulent, det kan holde med at vedkommende holder til i en annen avdeling enn den avdelingen hvor analysen foregår. I referanse B derimot blir det ikke nevnt at det kan være bra å få inn utenforstående til å sjekke arbeidet. Det nevnes bare at en trenger personer som skal utføre analysen. Å ha den riktige kompetansen tilgjengelig er såpass viktig at dette punktet var verdt å nevne. En fallgruve ved å kun ha noen få interne ressurser er at ting da kan ende opp med å ikke bli objektive nok, for eksempel ved hendelser som er innrapportert som angår personer som er med på analysen.

3.1.3 Identifisering av uønskede hendelser

I referanse A beskrives det kort hva en uønsket hendelse er og hvordan de uønskede hendelsene kan klassifiseres (jf. kapittel 2.1). Det blir i tillegg nevnt at de uønskede hendelsene må gi informasjon om hvilke verdier som berøres og hvor hendelsen kan inntreffe. Som eksempel har Datatilsynet gitt følgende;

«… uønsket, permanent utlevering av kundeopplysninger via e-post systemet …», (Datatilsynet, 2002)

Utover det som er nevnt over har ikke Datatilsynet lagt ved noen beskrivelse på hvordan de uønskede hendelsene kan bli identifisert. Så om en her bruker enkle metoder som diskusjon og brainstorming, eller om det tas i bruk mer formelle teknikker som for eksempel HAZOP, blir opp til personellet som gjennomfører risikovurderingen.

Risikovurderingen av informasjonssikkerhet hos en kommune, referanse B, gir heller ikke mye informasjon om hvordan en best kan identifisere uønskede hendelser. I referanse B oppfordres det til å samle hele gruppen som er delaktig i risikovurderingen for så å samlet gå gjennom en rekke trusler/uønskede hendelser som er vedlagt referansen. Vedlegget er i form av en trusseltabell hvor alle trusler, som enten gruppen kommer på selv eller som allerede er plassert der av NST, må gjennomgås.

Når det gjelder referanse C, Finanstilsynet, blir ikke uønskede hendelser identifisert direkte slik som nevnt i referanse A og B. Ettersom dette er en rapport over hvordan året som var har gått så presenteres ulike funn og observasjoner som Finanstilsynet har gjort. Disse funnene og observasjonene er deretter utgangspunktet for hvilke områder Finanstilsynet klassifiserer som risikoområder for det kommende året, og er dermed en form for identifisering av uønskede hendelser. De bruker altså erfaring til å beskrive uønskede hendelser. Finanstilsynet beskriver at hovedkilden til de funnene som er gjort er basert på innrapportering av hendelser fra foretakene, gjennomføring av IT-tilsyn, intervjuer med ansatte i foretak og møter med foretak og leverandører.

Referanse D velger å dele uønskede hendelser inn etter hvilke farekilde hendelsen går inn under, disse kildene er *natural, human, environmental* og *system design*. For hver av disse kildene blir det gitt en matrise som viser de forskjellige truslene. Det blir ikke eksplisitt beskrevet hvordan analysen kommer frem til de forskjellige hendelsene eller truslene men en kan se at det er en del av de samme truslene som er nevnt som eksempler i risikostyrings-guiden fra NIST (National Institute of Standards and Technology), se (Stoneburner, Goguen, & Feringa, 2002). Det er derfor rimelig å anta at de i referanse D har brukt denne guiden som utgangspunkt og videre supplert med egne trusler.

Identifisering av uønskede hendelser er en kritisk del av en risikoanalyse, grunnen til dette er at dersom en ikke har identifisert en hendelse så kan hendelsen ikke bli håndtert videre. Som nevnt finnes det flere måter å gjennomføre denne identifisering på, i referanserapport B har

det blitt brukt ferdigdefinerte lister med supplering av egne hendelser. Faren ved at en for eksempel velger å ta i bruk ferdigdefinerte «standard-hendelser» når uønskede hendelser skal identifiseres, er at en da risikerer å utelate mange relevante hendelser. Det blir ofte nevnt at prosessen ved å identifisere uønskede hendelser skal være en kreativ prosess, det vil si at også «uvanlige hendelser» må identifiseres. I boken (Aven, 2008) skriver forfatteren at det er vanlig å bruke en såkalt 80 – 20 regel, det vil si at en kan bruke 20% av tiden til rådighet til å identifisere 80% av de uønskede hendelsene, dette vil da ofte være hendelser som er kjent fra før og som personellet har erfaring med. Videre skal en bruke 80% av tiden til å finne de resterende 20% av hendelsene, det vil si de unormale og uvanlige hendelsene.

I referanserapportene blir det ikke lagt noe vekt på å formidle at det ofte kan være krevende å finne frem til de riktige hendelsene. Som beskrevet gir rapportene inntrykk av at denne identifiseringen bærer preg av rutinearbeid. Det skal dog nevnes at referanse A gir noe mer inntrykk av at identifiseringen av hendelser er en viktig del av vurderingen kontra referanse B. Ved å gjøre som i referanse D, kategorisering av truslene innenfor fire hovedkategorier vil identifiseringsprosessen bli mer oversiktlig og det kan hjelpe til med fordeling av arbeid innad i gruppen. På den andre siden så kan denne kategoriseringen føre til at kreativiteten blir noe innsnevret slik at analytikerne blir for opphengt i de fire kategoriene.

For å gjøre arbeidet med identifisering noe mer strukturert enn hvordan det blir gjort i A og B, burde de kanskje ha tatt med en formell metodikk i tillegg til diskusjon og gjennomgang av predefinerte trusler. For eksempel kan SWIFT bli brukt til å identifisere uønskede hendelser. SWIFT står for *Structured What-if Technique* og går ut på å bruke spørsmålet *hva om* (what if) til å identifisere potensielle avvik fra normalstatus på systemet. Ved bruk av denne metoden kan analysegruppen lettere gå strukturert gjennom listen og dermed være mer sikre på at de viktige hendelsene blir plukket opp. Et annet moment som er viktig å få frem når det er snakk om hvordan uønskede hendelser skal bli identifisert er at personellet som gjennomfører identifiseringen ikke må bruke unødvendig mye tid, det vil si at det kan hende at personellet ser for seg at de skal identifisere «alle» mulige hendelser. Gjør de dette kan de risikere å gape over for mye arbeid slik at de viktige hendelsene ikke får den oppmerksomheten som er nødvendig. Dermed er det viktig å skalere arbeidet i forhold til formålet, er det en mindre analyse av et ikke-kritisk system som er beregnet til å ta en uke å utføre, skal ikke identifisering av hendelser gå over veldig mange dager.

Som nevnt kan det bli problematisk dersom hendelsesidentifikasjonen blir et rutinearbeid. Ofte vil analytikerne som utfører analysen ha gjort flere analyser på «liknende» systemer tidligere og da er det kanskje lett å bruke de identifiserte hendelsene fra forrige analyse. Dette er et punkt som er viktig å ha i tankene når analysen utføres, selv om systemene er «tilnærmet» like vil de som regel ha noen forskjeller som er viktig å registrere slik at alle potensielle uønskede hendelser kan bli identifisert.

Så for identifisering av uønskede hendelser i forbindelse med en risikoanalyse av et IT-system mener undertegnede at analysegruppen må sette seg ned og gjennomgå mulige uønskede hendelser, gjerne ved hjelp av SWIFT-analyse, det må være personell til stede med kompetanse på de forskjellige tekniske systemene da store IT-systemer kan være veldig komplekse. Kategoriser truslene etter de fire kategoriene som nevnt. En bør unngå å bruke ferdigdefinerte lister. Det bør også kommuniseres ut til alle deltakende at det er viktig å finne frem til hendelser som ikke er vanlige (ref. 80/20-regelen).

3.1.4 Årsaksanalyse

Når de uønskede hendelsene er identifisert følger årsaksanalyser for å gjør rede for hvordan disse hendelsene kan oppstå. Som for identifisering av uønskede hendelser finnes det flere måter å gjennomføre en årsaksanalyse, eksempelvis kan enkel brainstorming brukes, eller en kan ta i bruk mer formelle metoder som feiltre-analyser eller bayesianske nettverk. Fordelen med de to sistnevnte er at en ved hjelp av disse også kan fastsette sannsynligheten for at den uønskede hendelsen inntreffer.

I startreferansene A og B blir det ikke gitt noen forslag eller guideline til hvordan denne prosessen skal bli utført. I A forklares det kun generelt hva som er hensikten med årsaksanalysen hvorav i B har en, som nevnt tidligere, en ferdig utfylt trusseltabell som også inneholder årsaker for de nevnte truslene. Ettersom det oppfordres til å supplere den vedlagte tabellen i B med egne identifiserte hendelser, er det dermed nødvendig å kartlegge mulige årsaker til disse. Det gis derimot ingen retningslinjer for hvordan denne kartleggingen bør skje. Når det gjelder referanse C så er det innrapporterte hendelser som utgjør rapporten og disse er allerede «etterforsket» og årsakene funnet, det blir derfor ikke hensiktsmessig å si noe mer om årsaksanalyse i forbindelse med denne referansen. I referanse D blir ikke begrepet årsaksanalyse brukt direkte, det er derimot tatt i bruk sårbarhetsidentifisering som en kan se på i forhold til årsaker, her skal det identifiseres potensielle sårbarheter som kan resultere i at en identifisert trussel blir utøvd på systemet. Til å identifisere disse sårbarhetene blir det tatt utgangspunkt i etablerte standarder fra blant annet NIST.

Så hvordan utføre en årsaksanalyse best mulig? Bør årsaksanalyser i forbindelse med IT-risiko bygges opp og utføres annerledes enn for, si et rørsystem på en plattform? Hovedessensen med analysen er som nevnt å komme frem til mulige årsaker til de identifiserte uønskede hendelsene. I noen tilfeller vil årsaksanalysen blir delt opp i flere sub-analyser, et eksempel på dette er gitt i (Aven, 2008), her blir det sett på den uønskede hendelsen *frakoplet fra server*, under årsaksanalysen blir en årsak identifisert som *strømforsyning feiler*, videre vil det være lurt å se på en årsaksanalyse på hvorfor strømforsyningen feilet etc. En hovedårsak kan dermed ha flere underårsaker. Dersom en tar i bruk feiltre-analyse som nevnt over vil dette gi et klarere bilde på hva årsaken faktisk er, og i dette feiltreet kan en tegne inn underårsaker slik at årsakene blir mest mulig komplette. Det vil derfor være av fordel å bruke teknikker som feiltre eller bayesianske nettverk. Ofte vil det være nødvendig med flere ulike typer personell i en slik analyse ettersom det kan være ulike disipliner som må redegjør for ulike årsaker. Dersom en årsaksanalyse for et IT-system burde være ulikt fra en årsaksanalyse av et annet system, (for eksempel rørsystem) vil det ikke spille noen vesentlig rolle ettersom årsaken må kartlegges uavhengig om det er i forbindelse med en serverkrasj i et datarom eller om det er gasslekkasje på en plattform. Det som likevel kan nevnes er at å finne årsakene til problemer i et IT-system kan vise seg å være veldig krevende ettersom det også finnes virtuelle komponenter og delsystemer som må analyseres, ikke bare fysiske komponenter som for et rørsystem.

Det som er verdt å ta med seg er at det viktige i en årsaksanalyse er at en faktisk kommer frem til årsaken og ikke bare en del av denne. Målet er å kunne legge et grunnlag for fremtidig håndtering og tiltak. Dersom en tar for seg et eksempel kan dette belyse viktigheten av å utføre årsaksanalysen grundig. La oss se på den uønskede hendelsen «brannmur nede». Under årsaksanalysen finner analysegruppen ut at årsaken til at brannmuren gikk ned var at en tekniker slo av hovedsikringen til begge de redundante strømforsyningene i stedet for bare sikringen til èn av de to. Dersom nå gruppen sier seg ferdig med denne årsaken og noterer den ned som «menneskelig feil» vil de kanskje gå glipp av informasjon, og hendelsen kan oppstå igjen. For å gjøre denne årsaksanalysen komplett bør en se på *hvorfor* denne teknikeren gjorde feilen. Her kan en for eksempel se på om det var noe galt med rutinene teknikeren jobbet etter, eller om utstyret ikke var markert godt nok etc. Ved å identifisere årsaker som dette kommer en til rot-årsaken, som videre gjør det lettere for bedriften å håndtere slike hendelser og sørge for at de ikke oppstår igjen. En annen fordel med å identifisere rot-årsaken er at dersom, gjennom tidens gang, den samme rot-årsaken dukker opp på flere hendelser kan dette

hjelpe til å identifisere hvor bedriften må legge ned mer arbeid for å forhindre fremtidige uønskede hendelser, eksempelvis rutiner eller opplæring av personell.

Det vil altså være nyttig om årsaksanalysene som beskrevet i referanserapportene ble gitt noe mer prioritet, det vil si at detaljeringsgraden av analysene kunne vært noe høyere. Dersom det velges å legge ned mer arbeid i denne prosessen kan det være for det beste, både for resultatet av selve analysen i tillegg til miljøet analysen utføres i. Dette fordi årsaksanalyser har en tendens til å bli en analyse som utføres i sin helhet av analyseteamet som da ofte tar i bruk etablerte datagrunnlag for å si noe om årsakene som er identifisert. Dersom en legger mer vekt på årsaksanalysen og trekker inn personell fra ulike disipliner vil en, i tillegg til å få en bedre årsaksanalyse, kunne oppnå et bedre tverrfaglig samarbeid og analysen kan da bli en form for samlingspunkt og informasjonsutveksling, dette gjelder for så vidt gjennom hele risikoanalysen, (DNV & RF, 2002).

Dermed vil undertegnede gjennomføre årsaksanalysen ved at den riktige ekspertisen går gjennom de uønskede hendelsene og identifiserer årsakene til disse. Det vil som nevnt være en fordel å kunne strukturere årsaksanalysen slik at det går klar frem hva som er årsak til hva, og om det er underårsaker som er identifisert.

3.1.5 Konsekvensanalyse

Hver uønsket hendelse medfører mulige konsekvenser, i konsekvensanalysen er jobben å identifisere disse konsekvensene slik at et samlet bilde på risikoen kan bli gitt.

I referanse A blir det forklart hva konsekvensanalyse er men det gis igjen lite informasjon om hvordan best utføre en konsekvensanalyse. Det som i midlertid kommer frem i retningslinjene fra Datatilsynet er at konsekvensanalyse ofte går ut på å identifisere konsekvenskjeder, dette fordi det er viktig å komme frem til den endelige konsekvensen og ikke bare deler av denne. På den andre side er det viktig å få frem at en konsekvensanalyse raskt kan bli for omfattende og kreve for mye tid fra analysegruppen, så her er det viktig med en balanse slik at riktig detaljeringsgrad kan bli valgt. Utover dette blir det ikke gitt noen råd om hvordan konsekvensene kan identifiseres. Kanskje burde Datatilsynet lagt ved et forslag på hvordan de mener en konsekvensanalyse burde bli gjennomført, for eksempel ved bruk av et hendelses-tre.

I NST sin risikovurdering av informasjonssikkerhet i en kommune brukes fremdeles den ferdigdefinerte trusseltabellen, i tillegg til denne tabellen er det vedlagt en matrise som definerer konsekvenskategorier med kriterier. Arbeidet i referanse B blir dermed å gå

gjennom alle truslene i trusseltabellen og angi konsekvens til disse ved hjelp av matrisen. Måten som dette blir gjort på kan medbringe utilsiktede fallgruver, for eksempel så kan noen av de uønskede hendelsene som er definert føre til konsekvenser som ikke sammentreffer godt nok med definisjonsmatrisen slik at en konsekvens dermed bare blir valgt på måfå. En annen svakhet er at en risikerer at den endelige konsekvensen ikke kommer synlig nok frem. Dersom gruppen finner frem til en konsekvens for en hendelse i matrisen og velger denne, kan det for eksempel være at den valgte konsekvensen bare er en «forkonsekvens» og at den endelige konsekvensen dermed blir utelatt. Dersom man ser det fra den andre siden derimot så er bruken av matrisen kombinert med trusseltabellen en måte som systematisk gjennomgår alle truslene og angir en konsekvens til hver.

Referanse C bruker, som tidligere nevnt, ikke samme oppbygning som de resterende tre. I denne er det hendelser som allerede er inntruffet som blir sett på og dermed har de ikke lagt ved noen spesifikk konsekvensanalyse.

I den engelskspråklige referansen (D) brukes også en form for definisjonsmatrise til å definere størrelsesordenen på konsekvensene. Konsekvensene bygger på evaluering av tre aspekter (identifisering av det truede aktiva, identifisering av lokalitet og identifisering av omfanget av offentlig sikkerhet som berøres). Alle sårbarhetene som tidligere er identifisert i analysen blir deretter gjennomgått og angitt en konsekvens (høy, medium eller lav).

Så sett over ett er konsekvensanalysen en viktig del av analysen, dersom en legger for lite arbeid ned i å identifisere konsekvensene til de allerede identifiserte uønskede hendelsene kan en ende opp med et risikobilde som ikke representerer virkeligheten godt nok. Dersom en ikke kun tar i bruk matriser som brukt i referanserapportene kan en for eksempel bruke event-tre-analyse eller hendelses-tre-analyse. Fordelen ved bruk av en slik metode er at den gir et godt oversiktsbilde på konsekvensene hendelsen kan resultere i, og de former et godt utgangspunkt for kunnskapen som brukes til å angi sannsynlighet. Dersom en i tillegg har nok informasjon til å kunne angi sannsynlighet for hver delkonsekvens kan dette brukes til å komme frem til sannsynligheten for den endelige konsekvensen.

Ved å utføre en *dårlig* konsekvensanalyse kan en, som nevnt, ende opp med en risikoanalyse som gir et feil inntrykk og dermed kan føre til at feil beslutninger blir tatt. For å komme frem til de respektive konsekvensene er det ofte nødvendig med bruk av underliggende metoder og modeller som beskriver det fenomenet som faktisk er under lupen. Eksempelvis kan det ved konsekvensanalyse av en gasslekkasje være nødvendig med en CFD-simulering for å simulere

hvordan gassen oppfører seg etter utslipp og om denne antennes etc. Dette viser hvordan en konsekvensanalyse raskt kan bli meget omfattende.

Usikkerhet knyttet til de forskjellige konsekvensene bør også bli tatt med, ofte har en for lite informasjon om hva en uønsket hendelse kan medføre. I forbindelse med IT er det kanskje spesielt vanskelig å ha full kontroll på alle mulige konsekvenser, særlig om det snakk om store IT-systemer. Komplekse IT-systemer er bygget opp av veldig mange elementer og tilhørende prosesser som må være oppe for at systemet skal fungere. Eksempelvis kan en se på den uønskede hendelsen «brudd på redundant fiberførsel mellom to datasenter». I første rekke vil kanskje konsekvensen av denne hendelsen bli identifisert som *bortfall av redundans mellom datasenter X og Y*. Innenfor IT-verden blir ofte slike datasenter bygget opp og modifisert med tiden, så selv om denne hendelsen kun skulle bety bortfall av redundans kan det for eksempel tenkes at det fra gammelt av ligger statisk rutet trafikk på denne linken som da vil gå ned når fiberen brytes. Her er det altså usikkerhet inne i bildet når konsekvensene skal identifiseres. Usikkerhet har fått sitt eget avsnitt hvor noe teori og aspekter tilknyttet usikkerhet blir diskutert, leser refereres til 3.1.7.

3.1.6 Sannsynlighet

Fastsettelse av sannsynlighet er også en viktig del av en risikoanalyse, sannsynligheten for at de identifiserte hendelsene inntreffer må beskrives. I referansene A og B har de stort sett lagt ved samme mulige måter å definere sannsynligheter på, i utgangspunktet er det vanlig å bruke historisk data, i form av frekvens, til å kvantifisere sannsynligheten. Ofte har en derimot ingen historisk data å basere dette på, dette kan være fordi det er et nytt system (hvilket det ofte er) eller det kan være grunnet manglende innrapportering av uønskede hendelser. Som beskrevet i gjennomgangen har Datatilsynet og NST lagt ved andre metoder for å definere sannsynligheten, da med utgangspunkt i motivasjon eller letthet (se. Avsnitt 2.1 og 2.2).

I referanse D brukes begrepet likelihood, likelihood defineres i rapporten som et kvalitativt estimat på hvor suksessfullt et eventuelt angrep vil være. Det blir også notert i rapporten at likelihood ikke nødvendigvis reflekterer en nøyaktig sannsynlighet for et angrep.

I referanserapportene blir risiko beskrevet basert på sannsynligheter og konsekvenser, finnes det bedre metoder å fastsette denne sannsynligheten på? Er det noen fallgruver ved å fastsette den på metoder som blir brukt i referanserapportene? I de tilfeller hvor en har historisk data er det fordelaktig å bruke denne dataen ved fastsettelse av sannsynlighet, dette fordi en da kan

minimere den subjektive inputen som eventuelt måtte komme fra analytikerne. Dersom en derimot ikke har historisk data må en kanskje ta i bruk metoder basert på letthet eller motivasjon. Da risikerer en som nevnt at analyseteamet må komme med noe mer subjektiv vurdering av for eksempel letthet, dersom dette skulle bli brukt til å definere sannsynligheten i fravær av historisk data. Når dette er sagt skal det sies at dersom en legger ned litt arbeid i å definere de forskjellige sannsynlighetsnivåene, enten det er basert på letthet eller motivasjon, kan en likevel ende opp med et brukbart resultat.

Ved fastsettelse av sannsynlighet mener undertegnede som nevnt at dette til størst mulig grad skal være basert på historisk data.

3.1.7 Usikkerhet

For å synliggjøre at usikkerhet er et viktig moment å ta med når risiko blir vurdert har en i oppgaven valgt å lage et eget avsnitt for nettopp usikkerheten. Usikkerhet er som nevnt knyttet opp mot hvorvidt en uønsket hendelse inntreffer og hvilke konsekvenser denne hendelsen kan resultere i. Dermed kunne usikkerhet blitt tatt med under henholdsvis avsnitt om konsekvensanalyse og sannsynlighetstildeling, men velges heller å bli plassert i et eget avsnitt for å synliggjøre innholdet. Ettersom usikkerhet har vært i stor grad fraværende i referanserapportene A-D gjør oppgaven her et poeng ut av at dette bør tas med.

I det følgende vil teori angående usikkerhet bli presentert, hva er usikkerhet? Hvorfor er det viktig å ta høyde for usikkerhet når en ser på risikoanalyser?

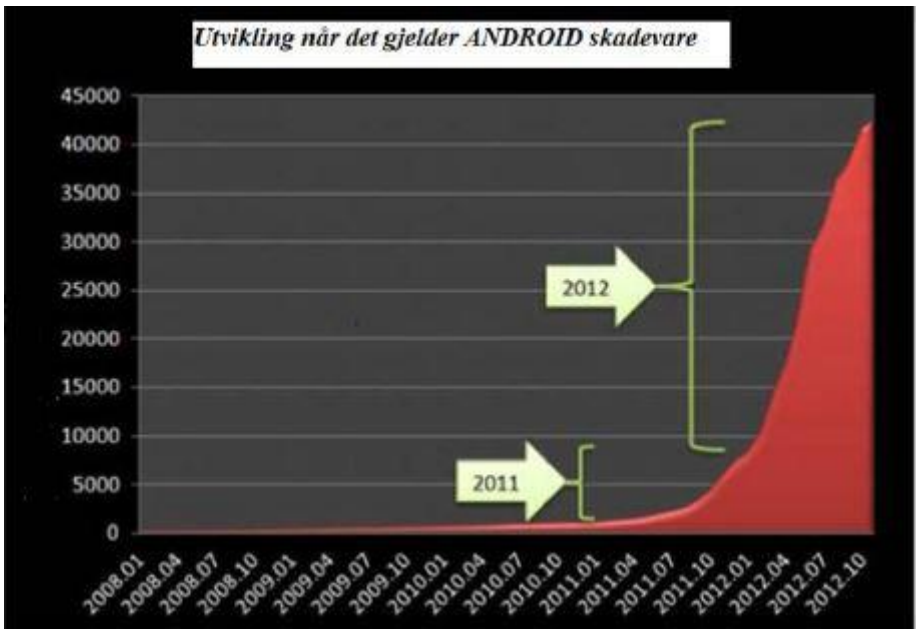
Hensikten ved bruk av risikoanalyser er å beskrive risikoen som analyseobjektet er utsatt for. Til å beskrive risikoen er det vanlig å ta i bruk følgende notasjon;

A	**Fremtidig hendelse**
C	Konsekvensen av denne hendelsen
U	Usikkerhet knyttet til om hendelsen A inntreffer og om hvilke konsekvenser C den kan medføre
P	Sannsynligheten for at hendelsen A inntreffer og at den spesifikke konsekvensen C oppstår
K	Bakgrunnskunnskapen som P og C er basert på

Tabell 5 Notasjon for risiko basert på (Aven, 2008)

Videre er det usikkerheten *U* som vil bli sett nærmere på. I (Aven, 2008) beskriver forfatteren at risiko ofte blir beskrevet ved hjelp av sannsynligheter og forventningsverdier. Videre nevnes det at det er viktig å vektlegge poenget om at ikke alle typer usikkerhet angående hva konsekvensene kan bli, reflekteres gjennom bruken av sannsynlighet. Dette fordi sannsynlighet er betinget en viss bakgrunnskunnskap som ofte er vanskelig å konvertere til sannsynligheter, (Aven, 2008)

Formålet ved å se på usikkerhet er i bunn og grunn å kunne gi et bedre beslutningsgrunnlag. Gjennom videre eksempler og diskusjoner vil det forsøkes å argumentere for hvorfor det nettopp er viktig å ta med usikkerhet. Som tidligere nevnt så har ikke, historisk sett, usikkerhet hatt mye plass i risikoanalyser av IT-systemer (jf. startreferanser). Årsakene til dette kan være mange, men undertegnede mener at usikkerhet også må tas hensyn til når det blir sett på risiko i forbindelse med IT-systemer. Som nevnt tidligere kan noen av disse årsakene forklares med at IT-systemer tidligere kun var tilkoblet lokalt og ofte manglet internettilgang, mens i dag er alt tilgjengelig på nett og ofte benytter fjernlagring. Datakriminelle har nå altså mye mer å hente på et eventuelt datainnbrudd enn hva som var tilfellet for eksempelvis kun 10 år siden. Et eksempel på at økningen i datakriminalitet er stor kan sees av følgende graf, hvor grafen vise økningen i skadevare på mobil-operativsystemet Android.



Figur 5 Sakdevare for Android hentet fra (Finanstilsynet, 2012)

Et annet moment som kan være interessant å nevne her er det faktum at nye IT-systemer ofte bygges med ny teknologi og nye måter å gjøre ting på. Som et resultat av dette er det ofte ikke mye data tilgjengelig som kan brukes i analysen som dermed gir rom for usikkerhet i forhold til hvilke konsekvenser en hendelse kan få og ved fastsettelse av sannsynlighet.

I den samme boken (Aven, 2008) presenteres et kort eksempel som gir et godt bilde på hvilke problemstillinger en kan komme borti dersom usikkerheten ikke tas hensyn til. Eksempelet er i sin helhet hentet fra (Aven, 2008);

> *En bedrift som bedriver service og installasjon av data- og telefonkabler gjennomfører en større risiko og sårbarhetsanalyse (ROS) for å se på den uønskede hendelsen «brudd på nedgravd kabel». Bakgrunnen for analysen er at det har vært et antall hendelser hvor selskapets nedgravde kabler har blir brutt grunnet graving med gravemaskin. Som en del av denne ROS-analysen blir en konsekvensanalyse utført for å belyse de mulige konsekvensene hendelsen kan medføre. Analysen kommer frem til at konsekvenser kan variere fra et par kunder uten tjeneste til brudd på hovedkabelen mellom to store byer. Sannsynligheten for den mest kritisk konsekvensen, brudd på hovedkabelen inntreffer er kalkulert til å være veldig liten. Hvis nå analyse-teamet konsentrerer seg om de forventede konsekvensene, at noen få brukere blir uten tjenester, for så å spesifisere en sannsynlighet for denne hendelsen og deretter bruker denne informasjonen videre i analysen, vil en viktig del av risikobildet ikke bli tatt med når risikoen blir fremlagt nemlig at ved ytterste konsekvens kan hele kommunikasjonen mellom to store byer bli brutt.* (Aven, 2008)

Fra eksempelet over ser en hvor kritisk det faktisk kan bli dersom analysen kun konsentrerer seg om forventningsverdier og ikke tar med usikkerhet i beregningene. Dette er som tidligere nevnt veldig vesentlig i dagens voksende IT-samfunn. Outsourcing blir mer og mer vanlig og kan medbringe store usikkerhetsmomenter. Ved leie/kjøp av IT-tjenester fra tredjepart har en ofte store og komplekse avtaler som skal dekke de fleste tilfeller og eventuelle hendelser som skulle dukke opp, likevel vil alltid være ting som en ikke alltid har kontroll over ved kjøp av slike tjenester. Ta for eksempel et IT-selskap som leier datakapasitet i India, denne tjenesten er viktig for selskapet og har derfor i tillegg leid en tilsvarende tjeneste i Spania for å kunne

ha full redundans. Plutselig går hele datasenteret i India ned som fører til at all trafikk blir kjørt mot Spania, som igjen fører til noe treghet for brukere. Hvis nå selskapet har tatt dette med som en uønsket hendelse i beregningene sine av risiko og gitt dette en lav risikoscore ettersom lokasjonen i Spania tar over og de trolig blir økonomisk kompensert for tjenesten i India, vil dette kunne gi et feil bilde på risikoen. La oss si at det viser seg at tjenesten i India gikk ned grunnet hackerangrep og det i ettertid viste seg at hackere har fått med seg brukerdata fra alle brukerne til selskapet. Eksempelet viser hvordan usikkerhet kan dukke opp og hvordan usikre momenter øker ved for eksempel komplekse systemer og outsourcing.

Videre kan en se på litt teori tilknyttet usikkerhet, usikkerhet deles ofte opp i to hovedgrupper, aleatorisk usikkerhet og epistemisk usikkerhet. Førstnevnte blir definert som usikkerhet som oppstår grunnet normale variasjoner i et systems ytelse og denne typen usikkerhet blir ikke redusert ved en eksperts rådgivning, det kan imidlertid nevnes at eksperters råd kan hjelpe til å kvantifisere usikkerheten (Hora, 1996).

Den andre typen usikkerhet, epistemisk usikkerhet, kan oppstå når det er mangel på kunnskap om hvordan et gitt system oppfører seg. Ettersom denne typen usikkerhet i hovedsak er mangel på informasjon kan usikkerheten reduseres og eventuelt elimineres ved tilfredsstillende studering av systemet (Hora, 1996). Dermed blir ekspertråd i forbindelse med epistemisk usikkerhet nyttig og kan eliminere usikkerheten, i motsetning til ved aleatorisk usikkerhet.

For å kunne ta med usikkerhet i risikoanalysen har oppgaven her tatt utgangspunkt i beskrivelse og inndeling av usikkerhet basert på (Abrahamsen, Aven, & Iversen, 2009). Denne artikkelen er laget som et rammeverk som tar utgangspunkt i å koble sammen gapet mellom sikkerhetsstyring og usikkerhetsstyring i petroleumsindustrien. Det blir brukt følgende kriterier for å fastsette usikkerheten:

Usikkerhetskategori	Beskrivelse av usikkerhet
Lav – 1	*Alle av de følgende kriteriene gjelder:* • Antakelsene som er gjort ved fastsettelse av sannsynlighet *P* og konsekvens *C* blir sett på som fornuftige. • Store mengder pålitelig data er tilgjengelig. • Det råder bred enighet blant eksperter.
Medium – 2	*Forhold mellom de som definerer lav og høy.*
Høy – 3	*En eller flere av de følgende kriteriene gjelder:* • Antakelsene som er gjort ved fastsettelse av sannsynlighet *P* og konsekvens *C* gir uttrykk for store forenklinger. • Data er ikke tilgjengelig eller pålitelig. • Det råder uenighet blant eksperter.

Tabell 6 Usikkerhetskategorier, hentet fra (Abrahamsen, Aven, & Iversen, 2009)

Nå som usikkerhetskategoriene er definert må en gå gjennom alle de identifiserte uønskede hendelsene som er med i analysen og gi disse en usikkerhetsscore som senere skal presenteres sammen med risikoscoren i en matrise. Som tidligere nevnt brukes her en definisjon på risiko som tar hensyn til fremtidige hendelser og konsekvensene til disse i tillegg til den tilhørende usikkerheten, dette er grunnen til at det har blitt valgt å legge en del vekt på usikkerhet i oppgaven.

For å tallfeste usikkerheten må en gå gjennom informasjonen som er tilgjengelig, og gjøre rede for informasjon som mangler eller er svak, for de respektive uønskede hendelsene. Her vil en, som nevnt, se på usikkerhet i forhold til (1) P(A|K) – sannsynligheten for at hendelsen inntreffer gitt bakgrunnskunnskapen K og (2) E(C|K) – forventet konsekvens gitt bakgrunnskunnskapen. En måte å gjennomføre denne tallfestingen er å notere all informasjon i en tabell som vist under, dette blir også brukt i andre avhandlinger, se for eksempel (Myrestrand, 2011). For å vise dette kan ta for seg eksempelet med brudd på redundant fiberførsel mellom datasenter A og B, som beskrevet tidligere.

ID	Uønsket hendelse (A)	P(A|K)	E(C|K)	U
XX	Brudd på redundant fiberførsel mellom datasenter A og B	Det er kjent at fiberkabler kan bli brutt som følge av små forstyrrelser på fiberen, i tillegg skjer det fra tid til annen at fiber blir gravd over av gravemaskiner etc. Fra historisk data og bakgrunnskunnskap blir det angitt en sannsynlighet på nivå på medium. (Som for enkelthetsskyld blir definert som 1 gang per 10 år)	Konsekvensene av hendelsen blir antatt å være små grunnet at det kun er en redundant link, men det er knyttet usikkerhet opp mot denne antakelsen, som nevnt tidligere kan trafikk ligge statisk rutet på linken som da kan i ytterste konsekvens føre til at kommunikasjonen mellom de to datasentrene går ned som igjen kan medføre nedetid for kunder (si at dette for eksempel var en ISP). Konsekvens = medium.	2

Tabell 7 Eksempel på beskrivelse av usikkerhet

Det nevnes også her at graden av usikkerhet må bli sett på i forhold til hvilken effekt den usikre faktoren har på konsekvensen. Det vil si at dersom en har høy usikkerhet og i tillegg høy effekt så vil dette bli definert som høy usikkerhet, dersom en derimot har høy usikkerhet men effekten på konsekvensen er lav vil dette medføre at usikkerheten blir plassert i kategorien lav eller medium. (Abrahamsen, Aven, & Iversen, 2009).

3.1.8 Visualisering

Visualisering er et punkt de fleste kan forholde seg til og ofte ha en mening om, og er nyttig i risikoanalyser. Med begrepet visualisering tenker en her på hvordan risikobildet eller resultatet av en risikoanalyse blir lagt frem, det vil si slik personer ser for seg resultatene. En mulig måte å legge frem resultatene fra en analyse er å ta i bruk risikomatrise. Som beskrevet i forrige kapittel er risikomatrisen et veldig vanlig verktøy som blir brukt i flere bransjer, eksempler er både referanse A og B. Et annet visualiseringsverktøy er *risikostige* som også kan brukes til å fremstille risiko. Dersom en først ser videre på matrisen, så gjør den at leseren lett kan finne frem til de hendelser som er viktige og hendelser kan raskt sees i forhold til akseptabelt risikonivå. Å bruke en matrise gjør det også mer intuitivt å forstå resultatene enn dersom resultatene bare hadde blitt beskrevet kvalitativt med tekst, slik som i referanse C. Dette kan en også se fra forskning, i (Medina, 2008) blir det sagt at den beste veien for å lære og for å huske er gjennom bruken av bilder og visuelle elementer, ikke gjennom skriftlig eller muntlig presenterte ord. I tillegg blir det sagt at en grafisk presentasjon av risiko kan i en

betydelig grad øke risikounngåelsen sammenliknet med en numerisk presentasjon av risiko, se (Stone, Parker, & Yates, 1997).

På den andre siden så er det aspekter ved bruk at risikomatrise, og andre visuelle elementer, som kan være problematisk i enkelte tilfeller. Dersom en for eksempel bruker forventningsverdien som en parameter i risikomatrisen vil en kanskje ende opp med et bilde som er for snevert til å gi den nødvendige informasjonen. Senere i oppgaven vil usikkerhet knyttet til blant annet forventningsverdi bli diskutert, men en kan allerede her legge vekt på at bruken av forventningsverdi kan resultere i at viktig informasjon kan bli utelatt i analysen. For eksempel en uønsket hendelse som har enorme konsekvenser blir utelatt fordi den tildelte sannsynligheten er mikroskopisk og forventningsverdien deretter ikke blir vesentlig. Selv om da forventningsverdien ikke blir stor betyr ikke dette at hendelsen ikke er verdt å ta med videre i analysen, hendelsen kan inntreffe selv om den nevnte forventningsverdien er lav. Det er altså av viktighet til helhetsbilde viktig å også ta med slike hendelser.

Sannsynlighet/ Konsekvens	Lav	Medium	Høy
Høy			
Medium			
Lav			

Figur 6 Eksempel på risikomatrise

Etter undertegnedes mening er det viktig å ta med en risikomatrise, eller andre visuelle innslag slik at resultatene kan vises med andre hjelpemidler enn bare tekst. Dette fordi resultatene fra en analyse eller vurdering i første omgang er til for å gi økt beslutningsstøtte, ofte til personell som ikke direkte har vært med på analysen, for eksempel ledelsen. For beslutningstakere er det viktig å kunne finne frem til den nødvendige informasjonen raskt og effektivt, noe som visuelle effekter er til hjelp med. Visuelle hjelpemidler skal også minimere rom for feiltolkninger, en god presentasjon av risikoen skal føre frem til samme tolkning enten det er en tolkning fra en analytiker som er med i analysegruppen eller det er driftsleder som kun ser den ferdige rapporten og matrisen. Ettersom teknologien stadig er i utvikling medfører dette også at mer avanserte visuelle elementer kan komme på banen som igjen kan være fordelaktig ved presentasjon av risiko.

Når dette er sagt så er det viktig å nevne at matrisen i seg selv ikke er veldig viktig, det har for eksempel liten effekt å ha en veldig dekorativ og grafisk avansert matrise dersom innholdet ikke er riktig. Til tross for at visualisering er viktig må en hele tiden ha i bakhodet at det er

innholdet i matrisen og arbeidet bak som faktisk er det viktige. Hvordan har analytikerne kommet frem til plasseringen av de forskjellige hendelsene i matrisen? Kan en være sikker på at plasseringen stemmer med virkeligheten? Spørsmål som dette kan kanskje være vanskelige å svare på, men det som er sikkert er at den visuelle fremstillingen kun er til nytte om det bakenforliggende arbeidet er utført korrekt.

I det kommende eksempelet (kapittel 5) har det blitt valgt å bruke en risikomatrise for å presentere resultatet av analysen. Dette fordi det skal være mulig å lese av resultatene raskt og effektivt, som nevnt over.

4 Gjennomføring

Hva er egentlig en god risikoanalyse? Finnes det et godt svar på dette spørsmålet? Er en god risikoanalyse et stykke arbeid hvor alle mulige kombinasjoner av hendelser, årsaker og konsekvenser er identifisert eller kjennetegnes en god risikoanalyse av noe annet? Hovedobjektivet til en risikoanalyse er å kunne gi et informativt bilde på hvordan risikobildet er, (Aven, 2008). En kan si at en risikoanalyse i seg selv ikke er verdt stort dersom den ikke blir brukt som et hjelpemiddel til beslutningsstøtte. Målet av en risikoanalyse er altså å kunne gi bedre beslutningsstøtte, dette kan være støtte til beslutningen om å installere et nytt ventilasjonssystem i en tunnel eller om en skal modifisere det som allerede er der. Et annet eksempel er ved design av et nytt IT-system hvor en analyse kan hjelpe å ta beslutningen for hvilken type strømredundans som er nødvendig.

Gjennom analysen skal potensielle problemer bli studert og håndtert før de inntreffer ved å redusere eller å eliminere sannsynligheten for at de oppstår i første omgang. Risikoanalysen er derfor kun et verktøy som skal hjelpe til å støtte opp under beslutninger, et viktig verktøy sådan. Ved valg av feil løsninger kan problematiske situasjoner oppstå som kanskje kunne ha blitt unngått om en skikkelig analyse var på plass før beslutningen om å gå for akkurat denne løsningen ble tatt. Dette kan være situasjoner som medfører ekstra kostnader, forsinkelser eller et unødvendig høyt risikonivå. I det følgende vil bruken av forskjellige verktøy bli diskutert og i første omgang grovanalyser.

4.1.1 Bruk av verktøy

Dersom en nå ser de fire ovennevnte referanserapportene over ett kan en si at disse hovedsakelig går i retning mot grovanalyser som da dekker identifisering av en uønsket hendelse, årsaksanalyse og konsekvensanalyse. En grovanalyse blir ofte gjennomført av et team bestående av 2 til 10 personer, som i referanse A og B ble det beskrevet at vurderingen ble utført av en mindre gruppe som satte seg ned for å jobbe sammen. Hovedmålet med en grovanalyse er i korte trekk å kunne få etablert et risikobilde med en relativt begrenset innsats, (Aven, 2008). Gjennomføringen av en slik analyse bruker ofte standardiserte dokumenter som består av tabeller med kolonner for hver av aspektene som analyseres, det vil si hendelser, årsaker, konsekvens og sannsynlighet. Så hvorfor bruke en grovanalyse?

Ved å gjennomføre en grovanalyse vil en som sagt komme frem til et grovt bilde over risikoen som er forbundet med analyseobjektet. Et slikt bilde over risikoen kan være en fordel å ha før en går i gang med grundigere analyser, dette fordi disse mer grundige analysene kan bli omfattende og dersom en må utføre en slik analyse for hele systemet kan det bli

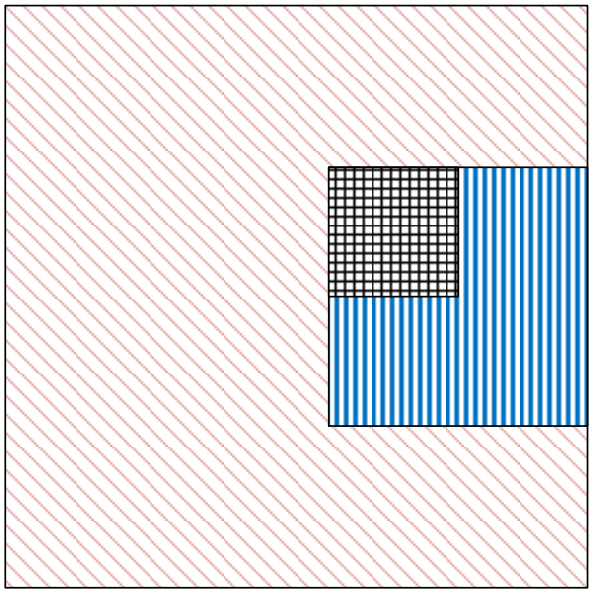
overveldende mye arbeid. Derfor er det lurt å først finne frem til hendelser som kan medføre risiko for så å bruke andre verktøy til å gå i dybden på disse. Når det gjelder IT-risiko gjelder også dette, ved for eksempel oppbygningen av et nytt IT-miljø kan en først gå i gang med en grovanalyse for å identifisere viktige risikoområder som videre kan bli analysert ved hjelp av andre verktøy.

Som beskrevet i noen av punktene kan en supplere analysene med for eksempel hendelsestre eller feiltre-analyser som da er eksempler på andre verktøy som er tilgjengelige. For å gjøre valget av verktøy noe mer intuitivt kunne det ha blitt laget et rammeverk for valg av verktøy i en gitt situasjon. I avhandlingen (Abrahamsen, Aven, Pettersen, & Tony, 2012) har forfatterne foreslått et rammeverk for valg av styringsstratgi i forhold til sikkerhetstiltak. I denne publiseringen legges det frem en stegvis prosess over hvordan en kan «guides» inn til bruk av riktig strategi gitt ulike utgangspunkt og vurderinger. Blant annet sees det på konsekvenser av en hendelse samt assosierte usikkerheter til denne, videre tas grad av overenstemmelse og eventuell tvetydighet i forhold til verdier med i den stegvise evalueringen. Til slutt kommer en frem til en foreslått strategi. I dette rammeverket brukes altså en stegvis prosess som skal komme frem til om det er mest nyttig å bruke en analysebasert tilnærming (som vil si en tilnærming basert på tradisjonelle risikovurderingsverktøy), en forsiktighets/føre-var-tilnærming (hvor tradisjonelle verktøy kan brukes men det legges opp til en stegvis lærekurve, dvs. at implementasjon kan stoppes underveis eller rulles tilbake ettersom problemer og ny informasjon kommer frem) eller en resonerende/forhandlingsbasert tilnærming (som vil si en tilnærming som legger vekt på deltakende beslutninger. Det nevnes at tilnærmingsmetoder fra de to foregående også kan brukes fordi det her skal velges tiltak som er basert på enighet, alle interessenter skal være med i diskusjonen.), se (Abrahamsen, Aven, Pettersen, & Tony, 2012).

Grunnen til at det er valgt å nevne den ovennevnte avhandlingen i oppgaven er at det viser at en ikke kan/bør bruke samme strategi i alle tilfeller, denne kunnskapen kan en videre se i forhold til bruken av risikoanalyser, og i første omgang grovanalyser, i forbindelse med IT-risiko. Det skal sies at bruk av grovanalyser kan være bra og i noen tilfeller være nok, men det en sikter til her er at en ikke i alle tilfeller kan bruke utelukkende en grovanalyse. For eksempel så kan en se, som tidligere beskrevet, at usikkerhet ikke tas opp nok i referanserapportene og i grovanalyser generelt. Som en initierende oppgave ved valg av analyseverktøy utover en grovanalyse kunne en for eksempel tatt en gjennomgang om det var store rom for usikkerhet knyttet til konsekvensene av en uønsket hendelse. Dersom det viste

seg at konsekvensene kunne sprike fra neglisjerbare til katastrofale, det vil si at forventningsverdien ikke burde bli brukt da den ofte skjuler usikkerheter, burde en umiddelbart tatt dette i betraktning og ikke bare gjennomført en «enkel» grovanalyse som ikke belyste denne problemstillingen.

Kombinasjonen av grovanalyse sammen med andre verktøy vil kunne være fruktbart, si at analysen starter med en grovanalyse som beskrevet over med uønskede hendelser, årsaker og konsekvenser. Som et resultat fra denne analysen vil en komme frem til noen områder hvor risikoen må bli analysert videre. Herfra tas usikkerhet med i vurderingen og som resultat fra dette punktet velger en så et (eller flere) verktøy til å gå videre i dybden på objektet. Tankemåten kan illustreres med følgende figur



Figur 7 Tankemåte

 - Initielt analyseområde, input til grovanalysen

 - Indentifisert risikoområde som resultat av grovanalyse, input til usikkerhetsvurdering

 - Identifisert risikoområdet når usikkerhet er tatt høyde for

Fra figuren over kan en se at grovanalysen hjelper til med å identifisere aktuelle risikofaktorer som igjen blir fokusert ved å ta hensyn til usikkerhetsmomentet. Ideen her er da å bruke andre tilleggsverktøy for å analysere de identifiserte områdene. Ved å gjennomføre risikoanalysen på denne måten vil en kunne være mer sikker på at tid og ressurser blir brukt på riktigt. Det

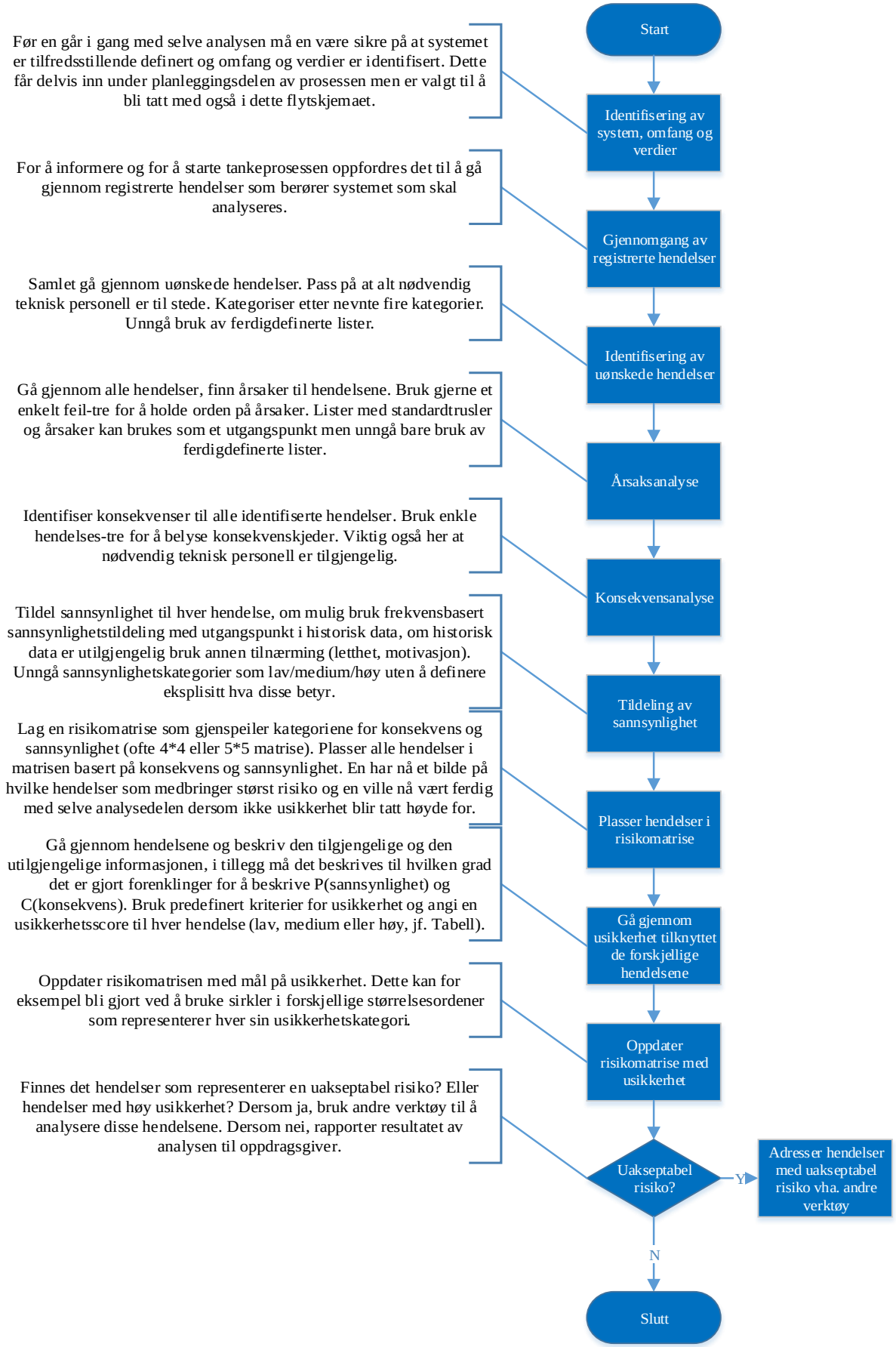
vil si at grundige analyser blir kun utført på deler av systemet som faktisk medfører en risiko. Det vil for eksempel være lite hensiktsmessig å gjennomføre en tidkrevende og avansert feiltre-analyse av en del av systemet som i grovanalysen er avdekket å ikke ha noen vesentlig risiko og usikkerhet knyttet til seg.

Tidligere i oppgaven har ulike verktøy blitt nevnt som kan benyttes i analysering og vurdering av IT-risiko, dette gjelder blant annet; grovanalyse, feiltre-analyse, hendelses-tre-analyse, SWIFT, FMEA, SJA, kost/nytte-analyse, bayesianske-nettverk med flere. Det er ikke innenfor omfanget til oppgaven å gå i detaljer gjennom alle verktøyene, likevel nevnes de for å vise at det finnes flere alternativer. For videre informasjon om hvert verktøy henvises leser til (Aven, 2008). Hvis en nå tar for seg IT-risiko igjen, hvilke verktøy er mest hensiktsmessig å bruke når det er risiko forbundet med IT-systemer? Svaret kan være noe vanskelig å gi, og en vil trolig komme frem til at valget av verktøy kommer helt an på omfanget og formålet med analysen. Det kan for eksempel være forskjeller på hvilke verktøy som trengs dersom man skal analysere og vurdere risiko i forhold til ny registreringstjeneste av matvarer på nett før en ankommer butikken kontra risiko forbundet med identifikasjonssystemet BankID som brukes ved identifisering og signering av tjenester på nett hos om lag 220 brukersteder (BankID, u.å.). Konsekvensene av en uønsket hendelse i matvareregistreringssystemet vil være mye mindre enn de potensielle konsekvensene av, si et sikkerhetshull i BankID.

Ettersom det er IT-risiko som her står i fokus kan det for eksempel være hensiktsmessig å ta en overordnet vurdering på systemets omfang før en går i gang med en risikovurdering. Som nevnt er det store variasjoner i kompleksiteten til et IT-system, noen system er enkle og blir driftet fra en enkelt server på en lokasjon mens andre systemer er bygget opp av flere undersystemer som ofte er geografisk plassert fra hverandre. I noen tilfeller, og i en økende grad er det også deler, om ikke hele, IT-systemer som blir outsourcet til andre land som for eksempel India, dette for å senke driftskostnadene. Med en gang en begynner med outsourcing av systemer åpnes det for andre typer uønskede hendelser og andre konsekvenser, det vil kanskje oppstå uoverensstemmelse mellom eier og drifter i forhold til verdier etc. Så hvilke verktøy er egnet i hvilke situasjoner? Her kan en komme tilbake til rammeverket nevnt over og kanskje bruke dette som utgangspunkt til å lage et tilsvarende for IT-risiko. Som et videre arbeid fra oppgaven kan det være av interesse å kunne ta i bruk nevnte rammeverk eventuelt lage et tilsvarende skreddersydd for IT-risiko.

4.1.2 Flytskjema

For å oppsummere hvordan en i kapittel 5 vil gjennomføre risikoanalysen følger på neste side et flytskjema som oppsummerer deler av diskusjonene over. Dette skjemaet er ment som et forslag til rammeverk hvordan en IT-risikoanalyse kan bli gjennomført.



Figur 8 Flytskjema av risikoanalyse av IT-system med usikkerhet

5 Eksempel

For å se på hvordan noen av funnene fra gjennomgangen av rapportene fra industrien kan eksemplifiseres vil en i dette kapittelet se på risikoen knyttet til inntoget av *IOT*. Ettersom IOT er et vidt begrep vil det i det følgende bli presentert avgrensninger slik at mengden informasjon ikke blir overveldende og at de ønskede poengene kommer til syne. Det må likevel legges trykk på at resultatet fra selve analysen ikke er hovedfokus i oppgaven. En vil se på hvordan analysen kan belyse aspekter nevnt under gjennomgangen av rapportene og i første omgang vise hvordan usikkerhet kan spille inn i bildet.

Det følgende eksempelet vil være som en mal for hvordan en kan vurdere risiko forbundet med IT og kunne opptre som en guideline til dette.

5.1 Tingenes internett

Forkortelsen IOT står for *internet of things*, eller *tingenes internett* på norsk, noen ganger blir det også referert til som *internet of objects* eller *internet of all things*. Begrepet ble først brukt ved Massachusetts Institute of Technology (MIT) da det ble arbeidet på deres Auto-ID Center som ble grunnlagt i 1999. Senterets arbeidsområdet var radio-frekvens identifisering (RFID) og sensorteknologier, se (Evans, 2011).

Tingenes internett rommer et stort antall begrep og ulike definisjoner, men er hovedsakelig at ting og objekter blir knyttet til internett og kan kommunisere med mennesker og hverandre. Det er lite tvil om at tingenes internett kommer til å forandre verden.

5.1.1 Avgrensning

I det følgende vil risikoen knyttet til en del av tingenes internett bli sett på. Grunnen til at det er valgt å se kun på et delsystem er kompleksiteten og at fokus fremdeles skal ligge på metoden å analysere risiko på. Delsystemet som vil bli sett på er de deler av tingenes internett som omhandler personlig elektronikk og i all hovedsak er tilknyttet personen eller hjemmet, og ikke tradisjonelle datamaskiner etc. Inn under denne avgrensningen tar en med ting som allerede er på markedet og har ikke fokus på fremtidig utvikling innen området.

For å være noe mer presis så vil følgende være med i avgrensningen;

- Internettilkoblede/smarte husholdningsmaskiner og hjemmeelektronikk (vaskemaskin, kaffemaskin, Smart TV, smart kjøleskap, spillsystemer etc.)
- Styringsenheter for varme og lys
- Smarte låssystemer for dører og vinduer

Gitt denne avgrensningen kan det legges ved eksempler som ikke blir tatt med. Ting som også går inn under IOT er smarte biler, smart grid (strømnett), e-health og smart infrastruktur for å nevne noen.

5.2 Analyse

Analysemetodikken vil i første omgang ha en struktur og oppbygning som likner på noen av de som tidligere er gjennomgått (se kapittel 2). Det presiseres her at hovedmålet ikke er å komme frem til et komplett risikobildet av IOT, men snarere å bruke risiko relatert til IOT for å vise poenger i forbindelse med oppbygningen av analysen. Først vil kartlegging av verdier følge, deretter vil eksempler på registrerte hendelser, som kan relateres eller delvis relateres til tingenes internett, bli presentert. Videre følger identifisering av uønskede hendelser, analyse av årsaker og analyse av konsekvenser. Hver hendelse vil deretter få tildelt en sannsynlighet før resultatet oppsummeres og publiseres grafisk i en risikomatrise.

5.2.1 Kartlegging av verdier

For enkelhetsskyld kalles innholdet fra avgrensningen over nå for *Smart Hus*. Verdiene som da kan etableres vil være sikkerhetsfunksjoner, eiendeler, personlig data, personopplysninger som kan videre representeres ved å se på tap/skadepotensiale for enkeltmenneskers liv, helse, økonomisk tap, tap av anseelse eller integritet. (jf. Datatilsynet).

5.2.2 Registrerte hendelser

Som en del av analysen er det ofte interessant å se på relaterte hendelser som allerede er registrert. Her vil noen hendelser som er veldig nært knyttet til analysen bli beskrevet, i tillegg tas enkelte hendelser som ikke direkte kommer inn under avgrensningen over med, da disse også gir et klart bilde på den økende risikoen innenfor IT og derunder tingenes internett.

5.2.2.1 Phishing og spamutsendelse fra husholdningsapparater

Når antall internettilkoblede enheter øker, øker også antall mulige mål for cyberkriminelle. I januar 2014 publiserte internettsikkerhetsselskapet Proofpoint INC. en pressemelding (Proofpoint, 2014) hvor de skriver at de for første gang kan bekrefte et angrep fra enheter som ikke er vanlige datamaskiner eller tablets. Angrepet bestod av rundt 750 000 falske e-postmeldinger hvor rundt 25% av disse kom fra ting som går under IOT-begrepet, nettverksroutere, Smart-TVer og smarte kjøleskap (Proofpoint, 2014). Angrepet i seg selv var ikke veldig farlig for den vanlige mannen i gata men dette rapporterte tilfellet bekrefter at sikkerheten rundt inntoget av IOT ikke har stått godt nok i fokus. Det ble bekreftet at mange av «deltakerne» i angrepet (det vil si den uskyldige tredjepart) ikke hadde blitt utsatt for et sofistikert angrep i forkant som gjorde det mulig å benytte smarte TV-er og kjøleskap til denne type formål. De kriminelle har snarere kun utnyttet at disse enhetene ofte ikke var konfigurert riktig og stod med standard-passord. Ved bruk av standardpassord vil enheten stå «åpen» ut mot internett og dermed bli bytte for et slikt angrep. Denne type sårbarheter er ofte

vanlig ved introduksjon av nye ting til markedet, produsenter vil ha sine produkter i hyllene så fort som mulig og dermed blir sikkerheten ofte ikke prioritert. Hadde for eksempel produsenten av dette smarte kjøleskapet som stod for mail-utsendelsen krevd at kunden satte sitt eget passord ved installasjon så kunne hendelsen vært unngått.

5.2.2.2 Stuxnet

I juni 2010 rapporterte et IT-selskap i Hviterussland om ormen *Stuxnet* for første gang, ormen var laget slik at den spesifikt skulle angripe en type styringssystem som ble brukt til styring av atomkraftverk enten for strømgenerering eller uran-anrikning i Iran. Ormen var laget til å angripe en Microsoft Windows-basert applikasjon som ble brukt av styringssystemer laget av Siemens, den kunne bli spredt via internettilkoblete maskiner i tillegg til usb-minnepenner, (Kushner, 2013).

Fra hendelsen ser man at risikoen ved å ha systemer tilkoblet internett er tilstede og kan bli utnyttet til alt fra spam-utsendelse til komplett overstyring av styringssystemer. Hvem som stod bak stuxnet-ormen er fremdeles ukjent, men noen sikkerhetseksperter mener at ormen kan ha blitt utviklet av en insider i Siemens som da hadde detaljert informasjon om systemet. Andre mener at en hel nasjon står bak ormen grunnet den sofistikerte koden som ble utviklet, (Kerr, Rollins, & Theohary, 2010).

5.2.2.3 Heartbleed

I april 2014 ble det offentliggjort at OpenSSL har en stor sårbarhet ved bruk av SSL/TLS-kryptering, SSL/TLS-kryptering blir brukt til å sikre kommunikasjon med forskjellige internettjenester som e-post, web og VPN (heartbleed.com, 2014). Noe av det som gjør dette sikkerhetshullet meget alvorlig er at hvem som helst på internett kan utnytte servere som kjører den kompromitterte versjonen av OpenSSL-programvaren uten at dette blir registrert noen plass. Angriperen kan hente ut bolker på 64KB fra minnet til en server, her får angriper tilgang til avlytte kommunikasjon, stjele data eller å utgi seg for å være tjenester og brukere (NorCERT, 2014). Hendelsen har fått stor omtale i media ettersom mange av de store tjenestene på internett har blitt rammet, eksempelvis Google med sine undertjenester som Gmail, Youtube, Ebay, Dropbox og Netflix, se (Kolberg, Heggen, Solbu, & Tjelle, 2014).

Hendelsen viser hva en enkelt sårbarhet er i stand til å gjøre nå som flere og flere tjenester er nettbaserte, konsekvensene kan bli enorme dersom «riktig» data blir stjålet.

5.2.3 Identifisering av uønskede hendelser

Uønskede hendelser vil være hendelser som kan utsette etablerte verdier for risiko. Uønskede hendelser kan bli identifisert ved hjelp av ulike metoder. Her kan for eksempel strukturert idémyldring bli benyttet eller man kan ta i bruk mer etablerte teknikker som FMEA eller HAZOP. Identifisering av uønskede hendelser er en kritisk og viktig del av selve risikoanalysen, man må passe på slik at uønskede hendelser ikke blir utelatt, da ingen utelatte hendelser kan bli håndtert. Samtidig er det viktig at denne aktiviteten ikke blir en rutine slik at listen med uønskede hendelser bare blir kopiert fra forrige analyse til den neste, selv om systemet kanskje var liknende. Det er viktig at identifisering av hendelser tar hensyn til alle aspekter ved systemet som skal analyseres.

ID	Hendelse	Kommentar
1	• Uønsket utlevering av personlig informasjon	Uvitende eller vitende utlevering av sensitiv data og personopplysninger.
2	• Smarte husholdningsartikler utilgjengelig	Her defineres smart-enhet som smart-TV, smart kjøleskap, smart vaskemaskin etc. Ikke alarmfunksjoner.
3	• Fjernstyring av optisk (?) enhet	Enhet som inneholder et kamera blir fjernstyrt.
4	• Fjernstyring av alarm/låsmekanismer	Utenforstående tar kontroll over låsmekanismer eller alarmsystem.
5	• Fjernstyring av varme- og lysstyring	Utenforstående tar kontroll over varme- og lysstyring som er tilkoblet internett.
6	• Datatyveri	Tyveri av personlig data
7	• Alarmanlegg fungerer ikke	

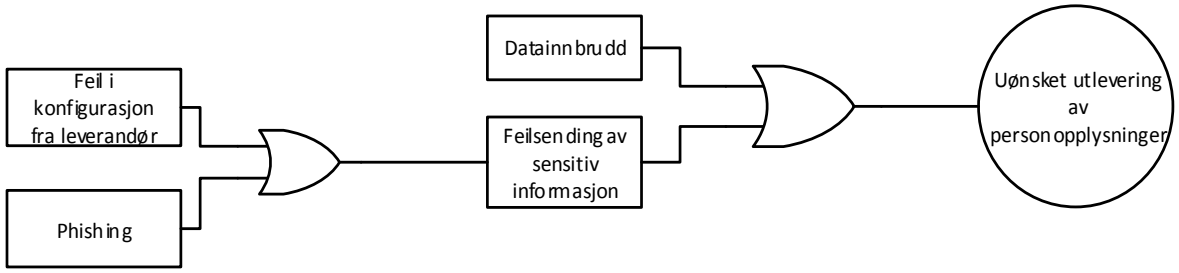
Tabell 8 Uønskede hendelser - Smart Hus

5.2.4 Årsaksanalyse

Som beskrevet tidligere i oppgaven følger årsaksanalyse etter identifisering av uønskede hendelser, her vil potensielle årsaker til de ovenfor beskrevet uønskede hendelsene bli beskrevet.

	Uønsket hendelse	**Årsak**
1	• Uønsket utlevering av personlig informasjon	- Feil i konfigurasjon - Datainnbrudd - Feilsending av informasjon
2	• Smarte husholdningsartikler utilgjengelig	- Feil i hardware - Feil fra leverandør
3	• Fjernstyring av optisk enhet	- Hackerangrep - Feil i konfigurasjon som gjør systemer åpne på nett
4	• Fjernstyring av alarm/låsmekanismer	- Hacking - Feil i konfigurasjon som gjør systemer åpne på nett
5	• Fjernstyring av varme- og lysstyring	- Hacking - Feil i konfigurasjon som gjør systemer åpne på nett
6	• Datatyveri	- Hacker skaffer seg tilgang til hjemmets lagringsenheter
7	• Alarmanlegg fungerer ikke	- Feil fra leverandør - Hardwarefeil

Som beskrevet i diskusjonen i kapittel 3 kan det være nyttig å ta i bruk for eksempel feiltre i forbindelse med analyse av årsaker. For å illustrere dette følger et feiltre for den uønskede hendelsen *uønsket utlevering av personopplysninger*.



Figur 9 Eksempel på enkelt feiltre

I figuren over kan en se hvordan et feiltre kan benyttes i årsaksanalysen til å belyse både årsaker og underårsaker. I eksempelet er det identifisert at årsaken til uønsket utlevering av personopplysninger er feilsending av sensitiv informasjon, videre blir dette undersøkt og det viser seg at denne feilsendingen igjen får to underårsaker. Her kan det for eksempel være en oppdatring av firmware fra leverandør som inneholder en feil i koden som gjør at feilen inntreffer. Den andre underårsaken, phishing, kan også medføre at for eksempel en bruker mottar en mail fra noe som utgir seg for å være noen andre, for eksempel en bank, fra mailen blir brukeren guidet til en falsk nettside hvor personopplysninger blir etterspurt.

5.2.5 Konsekvensvurdering

Ved å gjøre en konsekvensvurdering tar en utgangspunkt i de identifiserte uønskede hendelsene og prøver å komme frem til mulige konsekvenser en slik hendelse kan få, gitt at den inntreffer. Som Datatilsynet beskrev handlingen med så skal det her undersøkes og gi svar på spørsmålet *«hva medfører»*.

Som nevnt kvantifiseres også konsekvensene for å kunne gi et samlet risikobilde. Her har en brukt en relativ vanlig tilnærming.

- K = 1 – Ufarlig
- K = 2 – En viss fare
- K = 3 – Farlig
- K = 4 – Kritisk

	Uønsket hendelse	**Konsekvens**	**Kommentar**	**E(C|K)**
1	• Uønsket utlevering av personlig informasjon	Brukerens informasjon blir tilgjengelig på nett.	Settes til en viss fare	2
2	• Smarte husholdningsartikler utilgjengelig	Bruker får ikke brukt sine husholdningsartikler, kan resultere i utsatt klesvask og dårlig mat i varmt kjøleskap.	Konsekvensen vurderes til ufarlig da dette sannsynligvis kun går ut over daglige gjøremål.	1
3	• Fjernstyring av optisk (?) enhet	Kan resultere i overvåkning av hjemmet gjennom for eksempel kamera i TV	Konsekvens vurderes til farlig ettersom overvåkning i eget hjem ville vært meget kritisk.	2
4	• Fjernstyring av alarm/låsmekanismer	Åpning av ytterdør og desarmering av alarm kan medfører innbrudd	Konsekvensen er satt til kritisk grunnet dens kritiske natur.	4
5	• Fjernstyring av varme- og lysstyring	Unødig strømbruk	Settes til en viss fare	2
6	• Datatyveri	Kan miste personlig anseelse dersom privat data blir offentliggjort	Konsekvensen settes til ufarlig ettersom det her er snakk om data som bilder/filmer etc. Ikke personinformasjon	1
7	• Alarmanlegg fungerer ikke	Brannmelding eller innbruddsmelding blir ikke tilsendt sentral	Kritisk	4

Tabell 9 Uønskede hendelser Smart Hus

5.2.6 Sannsynlighetsvurdering

Som vist tidligere i oppgaven må en angi sannsynlighet for hver av de identifiserte hendelsene. I eksempelet defineres sannsynlighet basert på frekvens, det vil si antall ganger det forventes at hendelsen inntreffer.

S = 4	Meget sannsynlig	Defineres om hendelser som er forventet å inntreffe en gang per 0 – 1 år
S = 3	Sannsynlig	Inntreffer en gang per 1 – 10 år
S = 2	Mindre sannsynlig	Inntreffer en gang per 10 – 100 år
S = 1	Lite sannsynlig	Inntreffer en gang per 1000 år

Tabell 10 Sannsynlighetsdefinisjon

	Uønsket hendelse	**Kommentar**	**P (A|K)**
1	• Uønsket utlevering av personlig informasjon	Basert på liknende hendelser og den stigende sofistikerte cyberkriminaliteten er det rimelig å sette sannsynligheten til *P=3.*	3
2	• Smarte husholdningsartikler utilgjengelig	Basert på tilgjengelig data fra leverandører og på liknende hendelser er det rimelig å sette sannsynligheten lik 4.	4
3	• Fjernstyring av optisk enhet	Ettersom flere og flere enheter er utstyr med kamera og disse tilsynelatende kan bli utsatt for angrep vil det være rimelig å tildele en sannsynlighet på 2 ettersom det ikke er mye entydig data tilgjengelig.	2
4	• Fjernstyring av alarm/låsmekanismer	Alarm- og låsemekanismer vil trolig ha ekstra fokus på sikkerhet ved designing og av den grunn også kunne motså de fleste angrep. Det forventes likevel at ettersom det kan være mye å hente for kriminelle ved å kunne fjernstyre disse at dette kan inntreffe en gang per 10-100 år, P=2	2
5	• Fjernstyring av varme- og lysstyring	Her vil det være vanskelig å angi en sannsynlighet ettersom det her er snakk om ting som bare så vidt har kommet på markedet. Det en derimot kan si er ut i fra motivasjon så settes sannsynligheten til 2 da det vil være lite motivasjon for kriminelle i å fjernstyre varmestyring kontra andre ting.	2
6	• Datatyveri	Basert på tall fra sikkerhetsselskaper og informasjon fra relaterte	2

		hendelser settes også her sannsynligheten til 2.	
7	• Alarmanlegg fungerer ikke	Ettersom alarmanlegget kan slutte å fungere av forskjellige årsaker og noen av disse er relativt vanlige settes sannsynligheten til 3.	3

Tabell 11 Tildelt sannsynlighet for uønskede hendelser Smart Hus

Et punkt som er viktig å nevne ved bruk av tabeller som over er at det er viktig å notere ned all informasjon som blir diskutert av analysegruppen slik at en i ettertid kan gå tilbake i rapportene å finne ut grunnlaget for å tildele akkurat denne sannsynligheten. Dersom en for eksempel ikke noterer ned informasjon som dette vil en kunne lure på hvor si P(A|K)=2 kom fra.

5.2.7 Konsekvens kombinert med sannsynlighet

For å gi et grafisk bilde på kombinasjonen sannsynlighet/konsekvens brukes det her samme metode som i flertallet av rapportene som ble gjennomgått, nemlig matrise. I neste kapittel vil en se på hvordan denne matrisen kan justeres slik at også usikkerhet kan få plass i det helhetlige risikobildet. Under er de ulike hendelsene plassert i forhold til konsekvens og sannsynlighet i matrisen.

Sannsynlighet	**Konsekvensgradering**			
	Ufarlig 1	**En viss fare 2**	**Farlig 3**	**Kritisk 4**
Meget sannsynlig 4	**(2)**			
Sannsynlig 3		**(1)**		**(7)**
Mindre sannsynlig 2	**(6)**	**(3,5)**		**(4)**
Lite sannsynlig 1				

Figur 10 Risikomatrise for smart hus basert på (C,P)

Fra dette kan en se at det er hendelsene 4 og 7 som er de mest kritiske og trenger tiltak, hvorav hendelsene 1 og 2 ligger i den gule sonen. Dette ville vært resultatet av analysen dersom en hadde fulgt oppskriften fra referanserapportene (A,B og D), det vil si at risikodefinisjonen var sannsynlighet multiplisert med konsekvens. I dette eksempelet ønsker en derimot også å inkludere usikkerhet som følger i neste avsnitt.

5.2.8 Usikkerhet

Til å fastsette usikkerheten brukes kriterier som beskrevet i tabell 6. Informasjon om usikkerhet i forhold til (1) P(A|K) – sannsynligheten for at hendelsen inntreffer gitt bakgrunnskunnskapen K og (2) E(C|K) – forventet konsekvens gitt bakgrunnskunnskapen må plasseres og utgjøre grunnlag for å tallfeste usikkerheten.

ID	Uønsket hendelse (A)	P(A|K)	E(C|K)	Kommentar	U
1	Uønsket utlevering av personlig informasjon	Basert på liknende hendelser og den stigende sofistikerte cyberkriminaliteten er det rimelig å sette sannsynligheten til *P=3.*	Brukerens informasjon blir tilgjengelig på nett. =2	Fastsettelse av sannsynlighet er sterkt forenklet, lite pålitelig data tilgjengelig.	3
2	Smarte husholdnings-artikler utilgjengelig	Basert på tilgjengelig data fra leverandører og på liknende hendelser er det rimelig å sette sannsynligheten lik 4.	Bruker får ikke brukt sine husholdnings-artikler, kan resultere i utsatt klesvask og dårlig mat i varmt kjøleskap.	Basert på påliteligdata representerer ikke angitt sannsynlighet store forenklinger. Usikkerhet settes til lav	1
3	Fjernstyring av optisk enhet	Ettersom flere og flere enheter er utstyr med kamera og disse tilsynelatende kan bli utsatt for angrep vil det være rimelig å tildele en sannsynlighet på 2 ettersom det ikke er mye entydig data tilgjengelig.	Kan resultere i overvåkning av hjemmet gjennom for eksempel kamera i TV	Det er lite tilgjengelig data fra liknende hendelser, fast-settelse av sannsynlighet gir derfor noe inntrykk av forenkling. Usikkerhet settes til medium	2
4	Fjernstyring av alarm/lås-mekanismer	Alarm- og låsmekanismer vil trolig ha ekstra fokus på sikkerhet ved designing og av den grunn også kunne motstå de fleste angrep. Det forventes likevel at ettersom det kan være mye å hente for kriminelle ved å kunne fjernstyre disse at dette kan inntreffe en gang per 10-100 år, P=2	Åpning av ytterdør og desarmering av alarm kan medfører innbrudd	Noe forenklinger i forhold til p. Lite tilgjengelig pålitelig data. Usikkerhet settes til medium	2
5	Fjernstyring av varme- og lysstyring	Her vil det være vanskelig å angi en sannsynlighet ettersom det her er snakk om ting som bare så vidt har kommet på markedet.	Unødig strømbruk	Her ansees antakelsene ved fastsettelse av sannsynlighet som fornuftige. Usikkerhet settes til lav	1

		Det en derimot kan si er ut i fra motivasjon så settes sannsynligheten til 2 da det vil være lite motivasjon for kriminelle i å fjernstyre varmestyring kontra andre ting.			
6	Datatyveri	Basert på tall fra sikkerhetsselskaper og informasjon fra relaterte hendelser settes også her sannsynligheten til 2.	Kan miste personlig anseelse dersom privat data blir offentliggjort	Antakelsene ift. P ansees som forenklet. Lite pålitelig data tilgjengelig. Usikkerhet settes til høy.	3
7	Alarm-anlegg fungerer ikke	Ettersom alarmanlegget kan slutte å fungere av forskjellige årsaker og noen av disse er relativt vanlige settes sannsynligheten til 3.	Brannmelding eller innbrudds-melding blir ikke tilsendt brannsentral.	Fastsettelse av sannsynlighet gir uttrykk for noe forenkling. Usikkerhet settes til medium.	2

Tabell 12 Usikkerhet

Fra dette kan en oppdatere risikomatrisen til å også inneholde usikkerhet. Her blir det brukt sirkler som et mål på usikkerheten til hver hendelse. Figuren er dermed inspirert av boblediagram som for eksempel brukt i (Chien, Lin, Chang, Tsai, & Uen, 2012) og i (Myrestrand, 2011).

Usikkerhet	Figur
1 - liten	
2 - medium	
3 - høy	

Tabell 13 Notasjon av usikkerhet til matrise

Videre oppdateres risikomatrisen med informasjonen fra tabell 11.

Sannsynlighet	Konsekvensgradering			
	Ufarlig 1	En viss fare 2	Kritisk 3	Farlig 4
Meget sannsynlig 4	(2)			
Sannsynlig 3		(1)		(7)
Mindre sannsynlig 2	(6)	(3) (5)		(4)
Lite sannsynlig 1				

Figur 11 Risikomatrise for smart hus basert på (C,U)

5.2.9 Diskusjon rundt eksempelet

Eksempelet ble laget for å illustrere hvordan en kan analysere risiko innenfor IT med også å ta med usikkerhet. Innholdet i eksempelet er til stor grad basert på undertegnedes meninger, det vil si at begrunnelser for valg av sannsynligheter etc. er gjort med den hensikt å illustrere i eksempelet, ikke for å kunne gi et reelt risikobilde av systemet smart hus. Dette ble også nevnt tidligere, at innholdet i analysen i seg selv ikke var vesentlig men snarere hvordan usikkerhet ble trukket inn.

Fra figur 11 ser en resultatet av analysen, her kan en se usikkerheten tilknyttet de forskjellige hendelsene. En kan for eksempel se at det er mye høyere usikkerhet knyttet til hendelse (1) enn hendelse (2). I en matrise basert på sannsynlighet og konsekvens, som ikke tok høyde for usikkerhet vil en se at disse to hendelsene ville blitt rangert likt. Dermed viser dette at en får mer informasjon til å basere en beslutning på ved å inkorporere usikkerhet, det vil si at beslutningsgrunnlaget blir bedre. Hendelse 1 var *uønsket utlevering av personopplysninger*,

her kan en se for seg at bruken av forventet konsekvens gjør utslag for usikkerheten. Selv om forventet konsekvens settes til at brukerens informasjon blir tilgjengelig på nett kan dette i ytterste konsekvens for eksempel føre til identitetstyveri dersom brukeren for eksempel bruker samme informasjon flere plasser, som er veldig alvorlig. Dette viser viktigheten og nytteverdien med å også bruke usikkerhet når risiko blir analysert.

6 Konklusjon og diskusjon

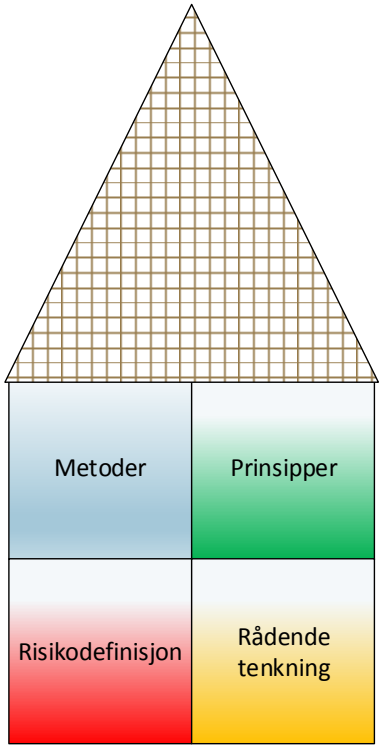
Utgangspunktet for oppgaven var å gjøre et studie over hvordan risiko blir sett på, analysert og vurdert innenfor IT-verdenen. Til dette ble det brukt fire referanserapporter fra ulike deler av industrien. Disse rapportene utgjorde videre et grunnlag for diskusjon som førte til forslag til hvordan IT-risiko kunne bli analysert. Dette forslaget var i form av et rammeverk som vist i figur 8. Rammeverket ble deretter utgangspunktet for eksempelet i kapittel 5.

Rammeverket som blir foreslått tar utgangspunkt i et IT-system hvor en har som mål å identifisere risikoområder. Første del gjennomføres som en grovanalyse hvor uønskede hendelser blir identifisert, det blir gjennomført årsaks- og konsekvensanalyse og sannsynlighet blir tildelt. Når dette er utført følger en grundig gjennomgang over hvilke usikre momenter som finnes. Dette er i førsteomgang knyttet til om det finnes usikkerhet rundt fastsettelse av sannsynlighet P(A|K) og forventet konsekvens E(C|K). For å definere usikkerheten blir det brukt kategoriene lav, medium og høy som defineres i tabell 6. En fastsetter usikkerhetskategori ved å se på mengde data tilgjengelig, grad av enighet blant eksperter og til hvor stor grad antakelser er fornuftige. Ved å plassere usikkerhet inn i samme matrise som en har sannsynlighet og forventet konsekvens får en frem hvilke hendelser som det er usikkerhet rundt, det vil si hvilke hendelser som er vanskelig å fastslå risikonivået til. Når så hendelser som medbringer stor risiko eller det er usikkerhet tilknyttet vil en kunne gå videre med bruk av andre verktøy, for eksempel feiltre-analyse, for å analysere disse hendelsene/områdene grundigere. Om en så har mulighet til å bruke andre verktøy videre vil selvsagt komme an på ressurstilgang, omfang og personell til rådighet.

En kan si at basert på de fire referanserapportene så blir risiko innen IT sett på som en kombinasjon av konsekvens og sannsynlighet, som beskrevet i kapittel 3.1.1. Oppgaven tar så videre for seg hvorfor denne måten å forstå risiko på kan være problematisk eller har rom for forbedring. Ved å endre synet på, og dermed definisjonen på risiko kan en bruke risikoanalyser til å gi mer og bedre informasjon enn tidligere, en vil dermed få et bedre beslutningsgrunnlag.

Når en risikoanalyse blir gjennomført så ligger det alltid et fundament eller et tankesett i bunn. Dette tankesettet er så utgangspunktet for hvordan hele analysen blir og hvordan en vurderer og forstår risiko. Et tankesett A vil medføre at risiko blir forstått på den ene måten mens tankesett B kan for eksempel se på risiko på en helt ny/annen måte. En kan se for seg dette fundamentet som en grunnmur i et hus, denne grunnmuren vil alltid være grunnlaget for

resten av huset og dersom grunnmuren endres vil også resten av huset måtte endres. Det kan også nevnes at ved en manglende eller en «uklar» grunnmur vil heller ikke huset bli bra, som da indikerer at resultatet av analysen vil bli mangelfullt. Grunnmuren er altså veldig viktig og en må være fullstendig klar over hvordan denne er bygget opp før en går videre i prosessen.



Figur 12 Grunnmuren i en risikoanalyse

Fra figuren ser en at risikodefinisjon er en viktig del av grunnmuren, oppgaven har gjennom eksempelet om smart hus forsøkt å kommunisere at måten IT-risiko i dag blir sett på burde bli endret. Forfatter av denne oppgaven mener at risikodefinisjonen som ligger til grunn i de nevnte referanserapportene ikke tar med en viktig dimensjon når det gjelder risiko, nemlig usikkerhet. Usikkerhet kan spille inn på mange områder i en risikoanalyse men i første omgang vil en trekke frem usikkerheten knyttet til konsekvens og forventet konsekvens samt tilhørende sannsynlighet. For det første så er det relativt vanlig å bruke forventet konsekvens som et mål når risiko analyseres. Det har tidligere i oppgaven blitt argumentert mot bruken av forventet konsekvens da forventet konsekvens i stor grad kan vike fra den faktiske konsekvensen. Dette er et moment som ikke kommer godt nok frem så lenge usikkerhet ikke blir tatt med i definisjonen. For det andre så er det også usikkerhet tilknyttet sannsynligheten som blir tildelt en hendelse. Sannsynligheten er bare et verktøy for å beskrive usikkerheten, og det som kan skape problemer her er at sannsynlighet er betinget en viss bakgrunnskunnskap, denne bakgrunnskunnskapen kan skjule usikkerheter, som beskrevet i

(Aven, 2008). Ofte vil det være vanskelig å finne nok data til å kunne tildele sannsynlighet objektivt, bakgrunnskunnskapen spiller som regel alltid en rolle. Mangel på data gjelder også i stor grad innenfor IT, det vil ofte være nye systemer som analyseres og en tar ofte i bruk ny teknologi som kommer med lite erfaringsdata. Ved å da kunne ta høyde for usikkerhet når en gjennomfører en risikoanalyse kan en synliggjøre usikre momenter som kan ligge skjult, og en vil dermed ende opp med en bedre analyse som igjen fører til et bedre beslutningsgrunnlag.

Selv om det er vanskelig å tallfeste usikkerheten vil det som regel gi et bedre grunnlag for beslutningsstøtte om en analytiker har tatt høyde for usikkerhet og av den grunn er mer bevisst på informasjon som mangler og hvilke usikkerheter som er til stede enn at analysen kun blir basert på forventet konsekvens med tilhørende sannsynlighet.

Tidligere i oppgaven ble det nevnt at den hurtige utviklingen av teknologi og IT-systemer kan være en kilde til usikre momenter, for eksempel outsourcing og cyberkriminalitet. Dette er et viktig poeng som støtter opp under argumentet for bruk av en definisjon på risiko som inkluderer usikkerhet. Som beskrevet tidligere i oppgaven var IT-systemer tidligere mye mindre og ofte var de uten internettilkobling. Etter hvert som tiden går har systemene endret seg drastisk og de fleste systemer er tilkoblet internett, dette utgjør en risiko med tilhørende usikkerhet. Et eksempel på *nye* risikoer som dukker opp er styringssystemer på offshore installasjoner som tidligere ble styrt av en operatør på installasjonen men som nå, etter hvert som IT-systemer utvikler seg, vil bli styrt fra land slik at styringen er tilkoblet internett, tenk på de konsekvenser det kunne få om kriminelle tok kontroll over styringssystem på en plattform. Her ville kanskje den forventede konsekvensen være at dette delsystemet som ble overtatt ble stengt ned for å fikse sikkerhetshullet, men hva om det samtidig med overtakelsen av systemet ble installert et virus som videre åpnet for fjernstyring av andre systemer da kunne konsekvensene blitt virkelig store. Det var her altså usikkerhet knyttet til den forventede konsekvensen.

Fra eksempelet tidligere gikk det frem at en ved bruk av usikkerhet i risikoanalysen vil en få mer nyttig informasjon ut fra analysen enn ved bruk av sannsynlighet*konsekvens-definisjonen. Konklusjonen på oppgaven vil derfor, i korte trekk, være at en innen IT burde gå over til bruk av en risikodefinisjon som tar høyde for usikkerhet.

Som en avsluttende del på oppgaven kan en se på hva som er kursen videre. Oppgaven kan bli sett på som et innledende studie innenfor bruken av IT-risikoanalyser som er basert på en risikodefinisjon som inkluderer usikkerhet. Kanskje det er dags for et tronskift på hvordan

risiko blir analysert og vurdert i IT-bransjen? Videre arbeid burde bli gjort for å videre studere gevinsten ved å introdusere usikkerhet og for å klargjør flere mangler ved å la usikkerhet utebli. Det vil da trolig komme klarere frem at analysen misser en del viktig informasjon når en ikke tar høyde for usikkerhetsdimensjonen.

7 Bibliografi

Abrahamsen, E. B., Aven, T., & Iversen, R. S. (2009). An integrated framework for safety management and uncertainty management in petroleum operations. *Summer Safety & Reliability Seminars - SSARS 2009*, 1-7.

Abrahamsen, E. B., Aven, T., Pettersen, K., & Tony, R. (2012). *A framwork for selection of strategy for management of security measures.*

Aven, T. (2008). *Risk Analysis - Assessing uncertainties beyond expected values and probabilities.* Wiley.

BankID. (u.å.). *Her brukes BankID*. Hentet fra BankID.no: https://www.bankid.no/Dette-er-BankID/her-kan-du-bruke-bankid/

Chien, T.-W., Lin, Y.-F., Chang, C.-H., Tsai, M.-T., & Uen, Y.-H. (2012). Using a bubble chart to enhance adherence to. *European Journal of Cancer Care*, 712-721.

COSO. (2004). *Enterprise Risk Management - Integrated Framework.*

Datatilsynet. (2002). *Risikovurdering av informasjonssystem.* Datatilsynet.

Department of Administration State Information Technology Services. (2011). *Risk assessment for altering and monitoring of the statewide microwave network.* State of Montana; Interoperability Montana; Lewis & Clark County.

Difi. (2010). *Veiledning i risikovurdering av elektronisk kommunikasjon.* Difi - Direktoratet for forvaltning og IKT.

DNV & RF. (2002). *Årsaksanalyse av prosesslekkasjer.* Stavanger.

Eilertsen, G. (2012). *Risiko og risikovurderinger - begreper og aspekter som er aktuelle ved tilsyn.* Trondheim: Utposten.

Finanstilsynet, T. F. (2012). *Risiko- og sårbarhetsanalyse (ROS) - Finansforetakenes bruk av informasjons- og kommunikasjonsteknologi (IKT).* Finanstilsynet.

heartbleed.com. (2014, April 29). *The Heartbleed Bug*. Hentet fra heartbleed.com: www.heartbleed.com

Henriksen, E., & Skipenes, E. (2013). *FUNNKe - Risikovurdering - Informasjonssikkerhet og personvern i elektronisk meldingsutveksling i pleie- og omsorgssektoren.* Nasjonalt senter for samhandling og telemedisin.

Hora, S. C. (1996). Aleatory and epistemic uncertainty in probability elicitation with an example from hazardous waste management. *Reliability Engineering and System Safety*, 217-223.

Justis- og Beredskapsdepartementet. (u.å.). *Trygg hjemme*. Hentet fra Justis- og Beredskapsdepartementet: http://www.regjeringen.no/nb/dep/jd/dok/nouer/2012/nou-2012-4/3/3.html?id=670720

Kerr, P. K., Rollins, J., & Theohary, C. A. (2010). *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability.* CRS Congressional Reseach Service.

Kolberg, M., Heggen, Ø., Solbu, E., & Tjelle, I. (2014, April 11). *Ikke bytt passord for tidlig*. Hentet fra NRK: http://www.nrk.no/norge/_-ikke-bytt-passord-for-tidlig-1.11660142

Kushner, D. (2013, Februar 26). *The Real Story of Stuxnet*. Hentet fra ieee spectrum: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Medina, J. (2008). *Brain Rules: 12 Principles for Surviving and Thriving at Work, Home and School.* Pear Press.

Myrestrand, M. (2011). *IT-risikoanalyse av offshoreinstallasjoner.* Brage.

NIST, National Institue of Standards and Technology. (2012). *Guide for Conducting - Information security.* Gaithersburg,: NIST Special Publication.

NorCERT. (2014, April). *Alvorlig sårbarhet i SSL*. Hentet fra Internettsikkerhet - NorCERT: https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Forsideartikler-NorCERT/Alvorlig-sarbarhet-i-SSL/

NST, Nasjonalt senter for samhandling og telemedisin. (2013). *Risikovurdering av informasjonssikkerhet.* telemed.no.

Petroleumstilsynet. (u.å.). *Risiko og risikoforståelse*. Hentet fra Petroleumstilsynet: http://www.ptil.no/risiko-og-risikoforstaaelse/category823.html

Proofpoint. (2014, January 16). *Proofpoint Uncovers Internet of Things (IoT) Cyberattack*. Hentet fra Proofpoint: http://www.proofpoint.com/about-us/press-releases/01162014.php

Stone, E. R., Parker, A. M., & Yates, F. J. (1997). Effects of Numerical and Graphical Displays of Professed Risk-Taking Behavior. *Journal of Experimental Psychology: Applied*, 243-256.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems.* Gaithersburg: NIST.

8 Figurer

9 Tabeller