2013

IKT SIKKERHET OG BEREDSKAP I TRE FYLKESKOMMUNER

Universitetet i Stavanger

Masteroppgave risikostyring og sikkerhetsledelse Høst 2013

UNIVERSITETET I STAVANGER

MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: **Høst 2013**

FORFATTER: **Anne Marit Staurheim**

VEILEDER: Kenneth Arne Pettersen

TITTEL PÅ MASTEROPPGAVE:
Hvordan oppleves IKT sikkerhet og beredskapsarbeid i tre av landets fylkeskommuner?

EMNEORD/STIKKORD:
IKT, sikkerhet, beredskap, risiko og sårbarhetsanalyse, øvelse, fylkeskommune.

SIDETALL:73

STAVANGER ……14.10.2013…….
DATO/ÅR

FORORD

Denne oppgaven markerer slutten på et langt studie. Gjennom fem år ved henholdsvis Høyskolen i Buskerud (HiBu) avdeling Drammen, og Universitetet i Stavanger (UiS).

Spesiell takk til Nasjonalt utdanningssenter for samfunnssikkerhet og beredskap (NUSB) i Heggedal med god tilrettelegging. NUSB har vært et utmerket sted for læring, hyggelig og nyttig bekjentskaper, spennende forelesninger og minneverdige stunder. Takk til alle mine forelesere og medstudenter.

En helt spesiell takk går til veileder Kenneth A. Pettersen ved UiS, takk for god veiledning og konstruktive og nyttige innspill gjennom hele oppgaven.

Stor takk til respondentene som deltok i min spørreundersøkelse. Uten dere hadde det aldri blitt noen undersøkelse.

Takk til Heidi, Tom Olav, Ingvil, Harald, Gølin og Ingrid som har kommet med gode og konstruktive innspill alle har bidratt hver på sin måte. Takk til Ole for at du gjorde dette mulig. Sist men ikke minst takk til deg kjære Elling for utholdenhet, stor tålmodighet og imøtekommenhet når min frustrasjon var som verst.

Arbeidet med masteroppgaven har vært en tidkrevende og arbeidsom prosess, men fremfor alt interessant, inspirerende og lærerikt!

INNHOLD

SAMMENDRAG

Informasjons- og kommunikasjonsteknologi (IKT) blir mer og mer aktuelt i alle virksomheter, dette er også gjeldende for fylkeskommunen. Oppgaven tar utgangspunkt i IKT sikkerhet og beredskap i tre forskjellige fylkeskommuner. Fylkeskommunene er omtrent like store i folketall, men geografisk spredt. Fylkeskommunen er ikke underlagt noe form for regelverk når det gjelder håndtering av intern IKT sikkerhet og beredskap. På bakgrunn av dette er det derfor interessant å se på hvilket fokus rådmann, IT leder og IT medarbeider har til IKT sikkerhet og beredskap. Felles for alle respondentene vil være at de vil bli berørt i forhold til oppgavens problemstilling.

Min hovedproblemstilling er følgende:
Hvordan oppleves IKT sikkerhet og beredskapsarbeidet i tre av landets fylkeskommuner?

Med «oppleves IKT sikkerhet og beredskap» menes i denne oppgaven: hvor godt forberedt man er til å håndtere en uønsket hendelse som resulterer i bortfall av data over tid med best mulig resultat. Dette omfatter ivaretagelse av alle fylkeskommunens funksjoner, slik at fylkeskommunen kan fungere best mulig som virksomhet dersom en uønsket hendelse skulle skje.
Fylkeskommunen er politisk styrt organ, og er en tjenesteyter til befolkningen i fylket. Det vil si befolkningen kan ikke velge bort den fylkeskommunen de sokner til, og heller velge en annen fylkeskommune. Dette gir noen utfordringer til kvalitet av leveranse.
Oppgaven er delt inn i fem temaer som følger hovedproblemstillingen. Disse er:

- Interne IKT lover og regler
- Sikkerhetsstyring
- Risiko og sårbarhetsanalyser (ROS)
- Beredskap
- Øvelse

For å beskrive IKT sikkerhet og beredskapsarbeid i disse tre fylkeskommunene, har jeg benyttet flere teorier og begreper som berører de fem temaene.
Datagrunnlaget for studien er innhentet ved å gjennomføre kvantitativ spørreundersøkelse, med relevante nøkkelpersoner som respondenter. I tillegg er det foretatt dokumentanalyse som måles og drøftes mot resultater fra (Mørketallsundersøkelsen™ 2012).
Spørreundersøkelsen og gjennomføringen beskrives nærmere i studiens metodekapittel. Presentasjon av funn presenteres i empiri delen, for videre å analyseres og drøftes i drøftingskapittelet. Videre oppsummeres og konkluderes funnene i det avsluttende kapittel.
En konkusjon av respondentenes opplevelse av IKT sikkerhets og beredskapsarbeidet i tre fylkeskommuner kan best beskrives som at det må gjøres en jobb for å forbedre dette arbeidet. Gjennom min oppgave har jeg avdekket flere faktorer som kan være årsak til at IKT sikkerhets og beredskapsarbeidet ikke får den oppmerksomhet det fortjener.

1 INNLEDNING

I dette kapittelet vil jeg forklare bakgrunnen for min problemstilling i oppgaven. Jeg vil si noe om hvilke temaer jeg ønsker å belyse, og hva oppgaven kan brukes til. Tilslutt i kapitlet vil jeg si noe om hvilke avgrensinger jeg har gjort, og hva jeg har funnet av tidligere forsking tilknyttet min problemstilling og tematikk.

1.1 Bakgrunn

De siste årene har vi gjentatte ganger blitt påmint hvilket sårbart samfunn vi lever i. Tragiske hendelser som terror og naturkatastrofer har bidratt til å synliggjøre at beredskapen på flere nivå i samfunnet ikke fungerer tilstrekkelig. God beredskap er en nøkkelfaktor for elektronisk kommunikasjon som er en nødvendig infrastruktur. Svikt eller bortfall av elektronisk kommunikasjonsnett og eller -tjenester vil kunne få alvorlige konsekvenser og skape store utfordringer for samfunnet, dette kommer fram av (Strategi for samfunnssikkerhet og beredskap i samferdselssektoren).

Informasjonsteknologi (IT) har skapt store endringer i samfunnet de siste tiårene. Gevinstene har vært betydelige for innbyggere, næringsliv og samfunnet som helhet. Informasjons- og kommunikasjonsteknologi (IKT) er blitt stadig mer integrert i alle deler av samfunnet, befolkningen får et bedre og mer mangfoldig tjenestetilbud. Man kan si teknologi utgjør grunnmuren for all samhandling på tvers av sektorer og opprettholdelse av samfunnets viktige funksjoner. Økt bruk av IKT gjør at samfunnet blir mer sårbart, truslene mot IKT systemene øker, og angrepene blir stadig mer avanserte. IKT har dermed blitt en strategisk sikkerhets utfordring. Infrastrukturen som ligger til grunn for at tjenestene fungerer, har blitt kritisk for at samfunnet skal fungere normalt. Blir det stadfestet i (Nasjonal strategi for informasjonssikkerhet)

Samfunnet har blitt mer sårbart for selv kortere driftsavbrudd i systemer og nett. Betydningen av en sikker og robust IKT-infrastruktur har således blitt større. Organisasjoner vil ikke kunne fungere optimalt uten IKT. Driftsavbrudd blir stadig mer kritisk, med driftsavbrudd menes brudd i data kommunikasjonen, som for eksempel ingen tilgang til fagsystemer eller dataområder. I noen tilfeller vil konsekvenser bli særdeles store, i dagens virksomheter blir økonomiske rammer blir stadig strammere og strammere. For å hente ut gevinster i organisasjonen er IKT infrastruktur og arkitektur i tillegg til effektive arbeidsverktøy grunnlaget for effektivisering. (Meld. St. 29, 2011–2012)

Ofte vil de fleste typer sikkerhetstiltak oppleves som plunder og heft i dagliglivet og ikke som nødvendig eller lønnsomt. *«Det har tidligere vært påvist et økende gap mellom trussel og sikkerhetstiltak. Trenden er at dette gapet fremdeles øker. Samtidig er det slik at verdien av samfunnets sensitive og skjermingsverdige informasjon øker.»* (Mørketallsundersøkelsen™ 2012. s.7) Undersøkelsen er blitt gjort av Næringslivets Sikkerhetsråd gjennom Datakrimutvalget, gjennom å foreta undersøkelse av norske virksomheter i privat og offentlig sektor med 5 ansatte eller flere.

Undersøkelsen er et viktig bidrag til å kartlegge omfanget av datakriminalitet og informasjonsteknologi (IT) sikkerhetshendelser, samt bevissthet omkring informasjonssikring og omfanget av sikringstiltak i norske virksomheter. Mørketallsundersøkelsen™ 2012 er den 8. i rekken og det 886 virksomheter som har besvart, noen av hovedfunnene i undersøkelsen er som følger:

- *«Av daglig ledere, som er øverste ansvarlige for sikkerhet og beredskap, svarer 1 av 5 at de ikke vet om det gjennomføres risikoanalyser i egen virksomhet.*
- *Bare 1 av 3 virksomheter har beredskapsplaner. Av disse igjen er det 1 av 3 som har krav til at det gjennomføres øvelser.*
- *12 % av de som har opplevd en hendelse har ikke fulgt opp med forbedringstiltak for å forebygge nye hendelser.*
- *Oversikt over hendelser er mangelfull på grunn av lite utbredt monitorering og logging i norske virksomheter, samt hendelsesrapportering til leder.*
- *Bare 1 av 6 virksomheter har retningslinjer for gjennomføring av verdivurdering.*
- *1 av 6 ledere vet ikke om det er utarbeidet en oversikt over virksomhetens personopplysninger.*
- *Bare 4 av 10 ansatte får opplæring ved nyansettelser. Av disse er det 4 av 10 som får kontinuerlig sikkerhetsopplæring. Dette til tross for at det er ansatte som oppdager flest hendelser, og eksterne angrep er ofte rettet mot ansatte og ikke teknologi.*
- *1 av 3 virksomheter vet ikke kostnaden knyttet til sikkerhetshendelser.»* (Mørketallsundersøkelsen™ 2012. s.9) (Næringslivets sikkerhetsråd 2012)

Med bakgrunn i denne undersøkelsen, st.meld. nr. 29 og tilsvarende rapporter, som alle viser til hvilket sårbart IKT samfunn iv lever i. Ønsker jeg å belyse fokus på IKT sikkerhet og beredskap i tre fylkeskommuner.

Man kan se på IKT som et nervesystem, som koordinerer aktiviteten til musklene, overvåker organene, modellerer og prosesserer input fra sansesystemene, og initierer handlinger. På lik linje kan man si IKT er nervesystemet i fylkeskommunen. Hele funksjonsevnen til fylkeskommunen er avhengig av IKT. Kollapser disse nervetrådene med IKT, så stopper alt opp. Konsekvensene av små bortfall av data er vi vant til å takle. Verre er det med bortfall over lang tid, eller enda verre med data som aldri kommer tilbake.

1.2 Problemstilling

Mitt forskningsspørsmål er:
Hvordan oppleves IKT sikkerhet og beredskapsarbeid i tre av landets fylkeskommuner?

Med «oppleves IKT sikkerhet og beredskap» menes i denne oppgaven: hvor godt forberedt man er til å håndtere en uønsket hendelse som resulterer i bortfall av data over tid. Dette omfatter ivaretagelse av alle fylkeskommunens IKT funksjoner, slik at fylkeskommunen kan fungere best mulig som virksomhet dersom en uønsket hendelse skulle hende.

Problemstillingen kunne vært knyttet opp til hvilket som helst organisasjon. Det som gjør fylkeskommunen så interessant er flere ting. Den er ikke underlagt noe lovverk fra myndighetshold å forholde seg til når det gjelder behandling av intern IKT sikkerhet og beredskap. Siden det ikke finnes noe form for lovverk vil det igjen si ingen tilsynsorgan fra myndigheters side, ei heller ingen veiledere som har fokus på fylkeskommunens interne IKT sikkerhet. Fylkeskommunen er politisk styrt organ, det vil si rådmannstillingen er som oftest besatt på åremål. Dette kan være en utfordring vedrørende strategi og langtidsplanlegging. Fylkeskommunen er en tjenesteyter til befolkningen i fylket. Det vil si befolkningen kan ikke velge bort den fylkeskommunen de sokner til, og heller velge en annen fylkeskommune. Dette fordrer kvalitet i leveranse.

1.3 Valg og begrensninger av oppgaven

Det er stort fokus på beredskap i virksomheter spesielt der liv og helse eller store økonomiske eller materielle verdier kan gå tapt. I slike virksomheter har ledelse og ansatte sikkerhet og risikohåndtering kontinuerlig på agendaen. Det investeres i teknologiske løsninger som skal forhindre og begrense ulykker, og det gjennomføres jevnlige beredskapsøvelser. Fokus på beredskap er som regel ikke så fremtredende i virksomheter som ikke er så utsatt. Fylkeskommunen er en slik virksomhet, som ved større svikt av IKT vil hverken liv eller helse bli berørt. Det vil derimot gå ut over sentrale funksjoner som offentlig tannhelsetjeneste, videregående opplæring, samferdsel, kultursatsing, næringsutvikling og tjenestetilbud til befolkningen.

Oppgaven omhandler hvordan IKT sikkerhet og beredskap er ivaretatt i tre av landets fylkeskommuner. IKT sikkerhet omfavner alt fra teknisk sikkerhet i datasystemene til opprettholdelse av virksomheten som virksomhet dersom en uønsket hendelse skulle skje. Det er det siste som denne oppgaven omhandler.

Jeg ønsker å få et bilde av fokus på interne lover or regler, sikkerhetsstyring, håndtering av beredskap og øvelser. Dette er blitt gjort gjennom å utarbeide en kvantitativ spørreundersøkelse for de forskjellige stillingsgrupperingene; fylkesrådmenn (leder), IT ledere (ansvarlige for IKT systemene) og IT medarbeidere (medarbeidere som har ansvar for drift og vedlikehold av IT systemene). Disse besvarelsene vil igjen bli sett opp mot funn i Mørketallsundersøkelsen™ 2012.

Oppgaven vil kunne brukes til å skape en større bevissthet rundt IKT sikkerhetsarbeidet. Som igjen vil kunne føre til mere robuste fylkeskommuner som kan håndtere uønskede IKT-hendelser med verst tenkelige utfall, med best mulig resultat.

1.4 Tidligere forskning

Sentrale myndigheter understreker i ulike offentlige dokumenter at både strøm og telenettet må gjøres mer robust enn det er i dag, for å tåle en krise, både elektrisk kraft og elektronisk kommunikasjon er definert som kritisk infrastruktur.

En spesiell aktuell rapport utgitt av Direktoratet for samfunnssikkerhet og beredskap (DSB) 2012, «Samfunnets sårbarhet over for bort fall av elektronisk kommunikasjon» hovedfunn viser: Tall fra kommuneundersøkelsen og data fra intervjuer viser at viktige beredskapsaktører er svært avhengig av ekomtjenester, men at de i liten grad har tatt hensyn til denne avhengigheten i planverk. Det er i liten grad gjort vurderinger knyttet til hvordan sårbarheten kan reduseres i egen organisasjon.

1.5 Oppgavens struktur

Kort beskrivelse av oppgavens struktur og innhold er som følger:

Kapittel 1: Omhandler bakgrunnen for min problemstilling i oppgaven. Jeg sier noe om hvilke temaer jeg ønsker å belyse og målet med oppgaven. Tilslutt hvilke begrensninger jeg har gjort og hva jeg har funnet av tidligere forskning når det gjelder min problemstilling og tematikk.

Kapittel 2: Omhandler fylkeskommunes historikk, hvor fylkeskommunen er plassert organisatorisk i forhold til det politiske hierarki. I tillegg beskriver jeg fylkeskommunens oppgaver og samfunnsmessige ansvar.

Kapittel 3: Omhandler forskjellige teoretiske tilnærminger til oppgavens problemstilling og hypoteser. Tilslutt i kapittelet vil jeg presentere mitt analytiske rammeverk som belyser ulike forhold som påvirker IKT sikkerhet og beredskapsarbeidet i fylkeskommunen.

Kapittel 4: Omhandler presentasjon av valg av metode, og hvordan den innsamlede data har blitt behandlet. Kapittelet er bygd opp slik: valg av metode for oppgaven, litt om hvilken data innsamling som er benyttet, valg av respondenter, beskrivelse av framgangsmåte for gjennomføring av spørreundersøkelsen. Avslutningsvis litt om validiteten og reliabiliteten i oppgaven.

Kapittel 5: Omhandler presentasjon av oppgavens kvantitative spørreundersøkelse og dertil funn.

Kapittel 6: Omhandler presentasjon av analyse og diskusjon av forskjellige teorier sett opp mot mine empiriske funn. Dette er igjen målt opp mot med funn i Mørketallsundersøkelsen 2012. Til slutt vil jeg oppsummere analysevurderingene ved å komme med noen konkrete utfordringer og tiltak for fylkeskommunen.

Kapittel 7: Omhandler presentasjon av konklusjon, og en kort oppsummering av min oppgave.

1.6 Nøkkelord

IKT, sikkerhet, beredskap, risiko og sårbarhetsanalyse, øvelse, fylkeskommune.

2 FYLKESKOMMUNEN

Dette kapitelet omhandler fylkeskommunes historikk, hvor fylkeskommunen er plassert organisatorisk når det gjelder det politiske hierarki. Det tar også for seg fylkeskommunens oppgaver og samfunnsmessige ansvar. Man kan tenke på fylkeskommunen som et stort tre, som har mange uoversiktlige greiner. Noen vokser fortere og er større enn andre, og noen knekker av eller dør og blir borte. Noen grener bærer store fine frukter og andre ikke. Lange inngrodde røtter som har lev i en årrekke og bukter seg alle veier. Man kan se på greinene og fruktene som forskjellige lokasjoner, avdelinger, prosjekter, oppgaver og tjenester. Noe av dette er mere synlig, nyttig og lønnsomt enn annet. Røttene er symbol på at fylkeskommunen er godt festet og inngrodd i det norske samfunn og dets funksjoner.

2.1 Kort historikk

Det er nitten fylkeskommuner i Norge, en i hvert fylke. det vil si hvert fylke unntatt Oslo utgjør en fylkeskommune. Dagens fylkeskommune fikk sin form så sent som i 1976. Denne formen ble til på grunnlag av en historisk utvikling gjennom flere hundre år. Etter 1814 ble folkestyret, demokratiet, en viktig drivkraft i forvaltningen. For å vite hva fylkeskommunen er, kan det derfor være nyttig å se tilbake i tid.

I vikingtida var Norge delt inn i fylker og skipreider, mindre områder som skulle stille et skip med mannskap til forsvar av landet. Fylkene ble først til len, med en lensherre som øverste embedsmann. I 1662 ble det bestemt at len skulle erstattes med det tyske ordet amt. Kongens mann ble nå amtmann, som tok seg av viktige lokale saker og rapporterte til København om amtets tilstand.

Norges løsrivelse fra Danmark og Grunnloven i 1814 førte til større åpenhet for lokalt folkestyre i Norge. Men det tok mange år og utredninger før Stortinget omsider samlet seg om et vedtak som er blitt kalt «Formannskapslovene av 1837». Disse lovene gjaldt den lokale forvaltningen av amt, kommuner og byer. Amtmannen skulle være den administrative leder av amtskommunen, og var det fram til 1976 (fylkesmann fra 1918).

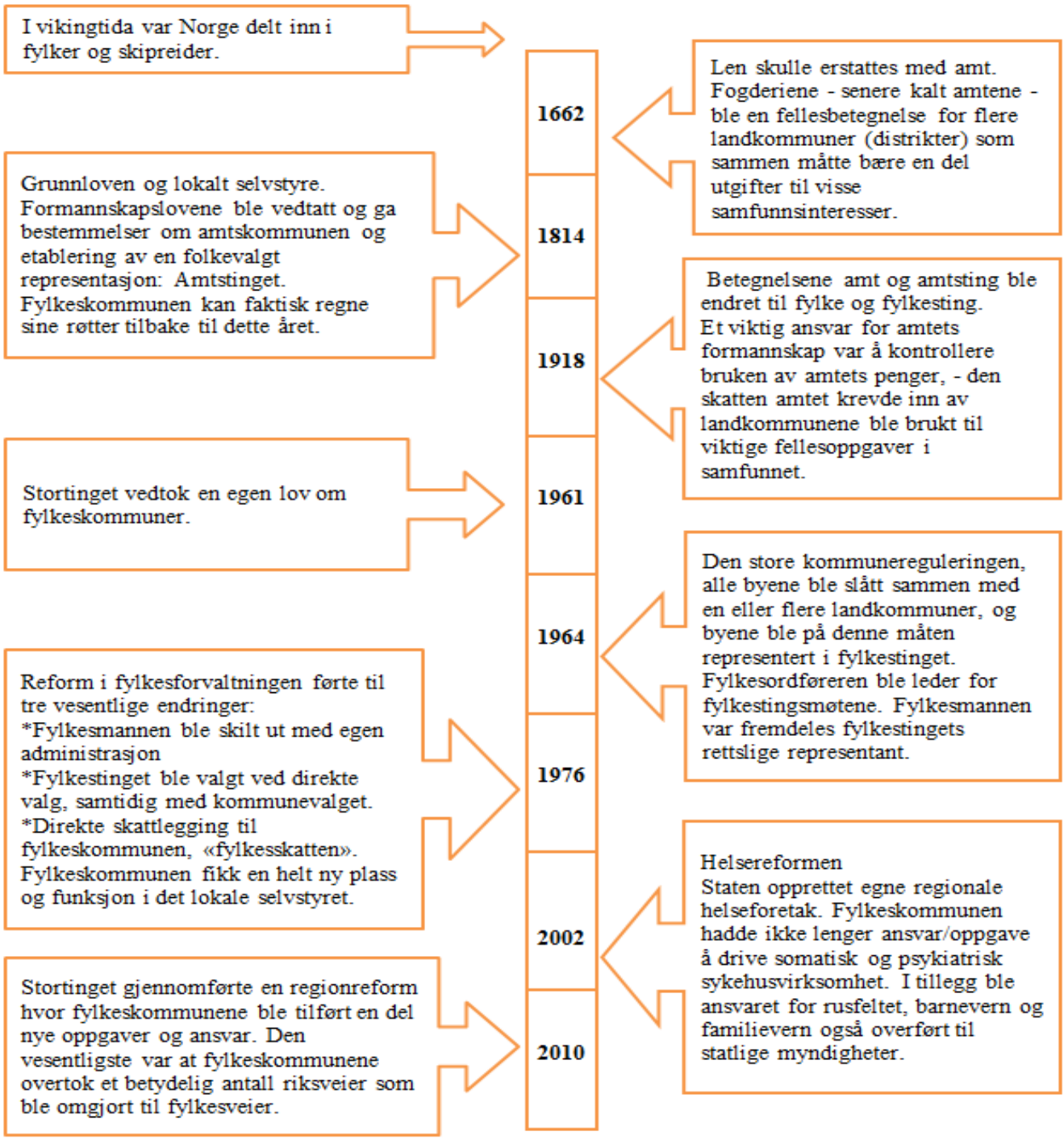
Det etablerte folkestyret med bystyrer, kommunestyrer og amtsformannskap (fylkesting) utviklet seg, men forble i prinsippet uforandret i mange år. Tiden var overmoden for reformer. To store samfunnsendringer skjedde da i løpet av kort tid: Kommunesammenslåingen i 1964 og reformen i fylkesforvaltningen i 1976.

Fylkeskommunens problemer med å leve opp til forventningene førte til en debatt om forvaltningsnivåets framtid, og det var sterke krefter som talte for å legge ned fylkeskommunen. En foreløpig avklaring kom med stortingsvedtaket i 2001 om at staten skulle overta sykehusene fra fylkeskommunene (helsereformen). Det skjedde med virkning fra 1.1.2002. Sammen med sykehusene flyttet også psykiatri og rehabiliteringstilbud.

Den viktigste endringen er at fylkeskommunen i større grad enn før skal være en "ledende regional utviklingsaktør". Fylkeskommunen deltar også i internasjonalt samarbeid innen

Norden og Europa. Parallelt med dette har fylkeskommunen beholdt ansvaret for å gi befolkningen et tjenestetilbud innen videregående opplæring, kollektivtrafikk, fylkesveier og tannhelse.

Figur 2-1 «Fylkeskommunens historie» viser de mest markante endringene i fylkeskommunens historie.



Figur 2-1 «Fylkeskommunens historie»

2.2 Dagens fylkesting og fylkeskommune.

Fylkeskommunen er det mellomste av de tre forvaltningsnivåene i Norge, og er styrt av fylkestinget. De to andre forvaltningsnivåene er kommune og stat.
Kommuneloven gir fylkeskommunene anledning til å velge politisk styringsmodell – fylkesutvalgsmodell eller parlamentarisk modell.

Fylkeskommunen er en demokratisk styrt organisasjon bestående av Fylkestinget. Fylkestinget består av folkevalgte representanter og ledes av fylkesordfører. Fylkesordføreren er den øverste politiske leder, mens fylkesrådmann (heretter kaldt rådmann) er den øverste administrative leder.
Delegasjonsreglementene beskriver hvordan fylkeskommunens makt og myndighetsutøvelse er fordelt i det politiske og administrative apparatet. Delegeringsreglementets formål er å fremme god saksbehandling og beslutningsadferd ved fordeling av vedtaksmyndighet. Reglementet skal videre sikre en hensiktsmessig oppgavefordeling, samtidig som behovet for reell politisk styring og kontroll, effektiv ressursutnyttelse og rettssikkerhet ivaretas.

Fylkestinget er det øverste politiske organet i fylkeskommunen og har ansvar for alle fylkeskommunale oppgaver. Fylkestinget gir vedtak på vegne av fylkeskommunen der det ikke er lov, forskrift eller delegasjonsvedtak. Innbyggerne velger nytt fylkesting hvert fjerde år. Noen sentrale oppgaver for fylkestinget er: fylkesplanlegging, økonomiplan og årsbudsjett.
Fylkestinget kan bestå av disse utvalgene:

- Administrasjonsutvalget som behandler saker som gjelder forholdet mellom kommunen som arbeidsgiver og de ansatte. De ansatte har representanter i dette utvalget.
- Forhandlingsutvalget som forbereder og gjennomfører forhandlinger/drøftinger med arbeidstakerorganisasjonene og enkeltarbeidstakere i saker der disse etter gjeldende lovverk og avtaleverk har forhandlingsrett.
- Hovedutvalg for kompetanse.
- Hovedutvalg for kultur.
- Hovedutvalg for næringsutvikling.
- Hovedutvalg for samferdsel.
- Fylkesutvalget (forbereder saker til fylkestinget).
- Kontrollutvalget fører løpende tilsyn med forvaltningen på egne vegne. Fylkestinget velger selv medlemmene.

Alle utvalg tilrettelegger saker innenfor sitt saksområde til fylkesutvalget. I saker som skal avgjøres av fylkestinget kan utvalget innstille en sak direkte til fylkestinget. Økonomi- og budsjettendringer gjøres via fylkesutvalget som innstiller til fylkestinget. I praksis ivaretar fylkestinget sitt ansvar ved å delegere oppgaver til fylkesutvalget, de faste utvalgene og til rådmannen, som på sin side delegerer videre myndighet til de ansatte i fylkesadministrasjonen.

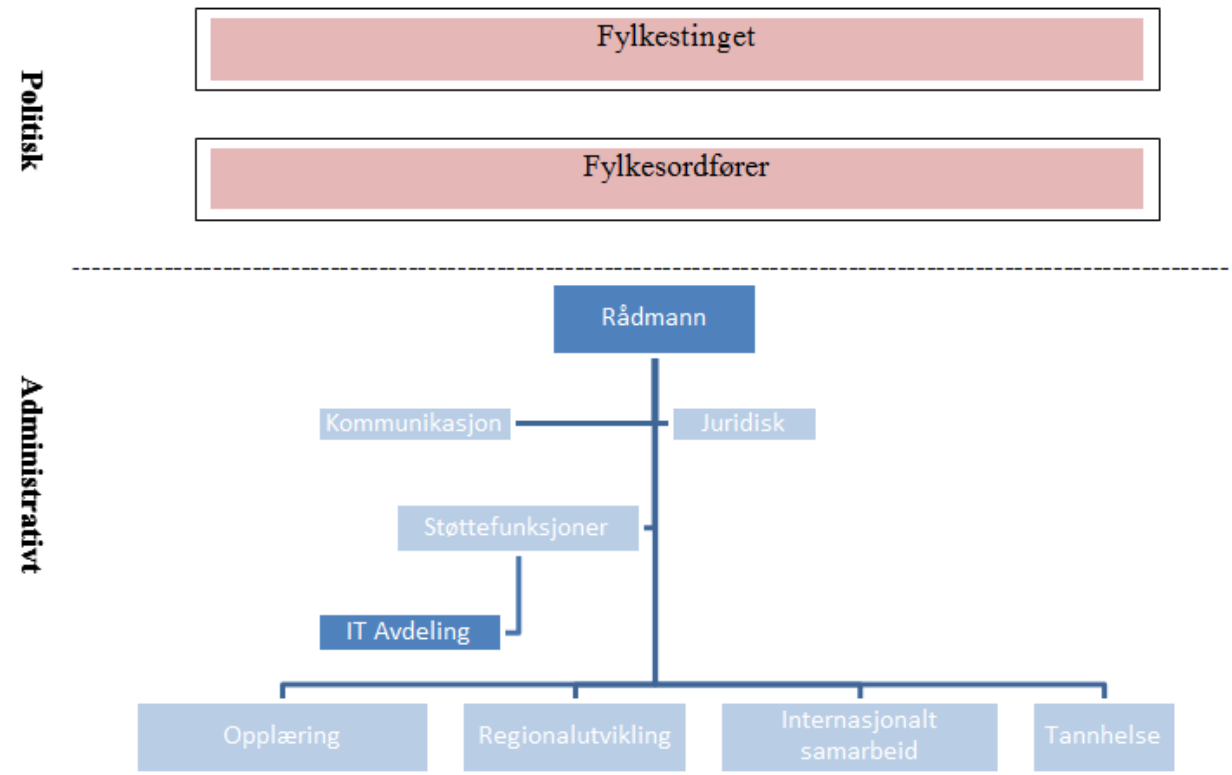
2.3 Fylkeskommunens organisering

De fleste av landets fylkeskommuner er organisert etter en tradisjonell fylkesutvalgsmodell. Kommuneloven krever at det i fylkeskommuner styrt etter den tradisjonelle modellen skal velges et fylkesutvalg. Med mindre det er grunnlag for flertallsvalg, krever loven at

fylkesutvalget skal sammensettes proporsjonalt når det gjelder fylkestinget. Kun medlemmer i fylkestinget er valgbare. Dette skal sikre at alle grupper av en viss størrelse blir representert i fylkesutvalget. Fylkesutvalget er gitt visse lovpålagte oppgaver, som behandling av årsbudsjett, skattevedtak og økonomiplan. Utover dette bestemmer fylkestinget selv hvilken myndighet, funksjon og oppgaver fylkesutvalget skal ha. I fylkeskommuner med fylkesutvalg skal det ansettes en administrasjonssjef som øverste leder for fylkeskommunens samlede administrasjon.

Som et alternativ til en fylkesutvalgsstyrt fylkeskommune kan det etter hvert bli flere fylkeskommuner som har innført et parlamentarisk styringssystem slik som Oslo og Bergen. Det er prinsipielt store politiske forskjeller på disse to måtene å organisere fylkeskommunen på. Kjernen i et parlamentarisk styringssystem er at administrasjonen i fylkeskommunen blir ledet av et politisk valgt kollegialt organ i stedet for en ansatt administrasjonssjef, og at dette organet er parlamentarisk ansvarlig overfor fylkestinget. I en slik modell velges det således ikke fylkesutvalg og det ansettes ingen administrasjonssjef i tradisjonell forstand. I stedet overtar et politisk organ, fylkesrådet, den øverste ledelse for fylkeskommunens samlede administrasjon. Rådet overtar også de oppgavene fylkesutvalget er pålagt gjennom lov. (St.meld. nr. 12, 2006-2007)

Studiet omhandler ikke den enkelte fylkeskommune, men alle tre sett under ett.
Hvert fylke unntatt Oslo utgjør en fylkeskommune, Oslo kan anses som en kommune eller fylkeskommune eller begge deler. Det vil derfor ikke bli noen beskrivelse av en organisasjon, men hvordan de fleste fylkeskommuner er organisert, tradisjonell fylkesutvalgsmodell som vist i Figur 2-2. Modellen viser fylkeskommunen fra politisk til administrativ organisering.



Figur 2-2 Fylkesutvalgsmodell modell.

2.4 Fylkeskommunens samfunnsfunksjon

Kommune og fylkeskommune er likestilte med ansvar for hver sine oppgaver. Fylkeskommunen har stort sett ansvar for det som går på tvers av kommunegrensene eller der den enkelte kommune ikke er stor nok til å løse oppgaven selv. Fylkeskommunen har ansvar for videregående opplæring, planlegging og støtte til kollektivtrafikk, anlegg og vedlikehold av fylkesveier, folkehelse, tannhelse, kulturminnevern, kultur og idrett, regional utvikling og regionalforvaltning. De største arbeidsområdene er videregående utdanning og offentlig tannhelsetjeneste. Fylkeskommunens overordnede mål kan beskrives slik:

- Fylket skal være et godt sted å bo, lære, arbeide og besøke.
- Økt verdiskapning og bærekraftig utvikling av fylket.
- Best mulig tjenestetilbud for folket i fylket.

Som nevnt tidligere i kap.1.3 er virksomheter som blant annet videregående skole og folketannhelse sine IKT systemer sentralisert noe som igjen gir mer effektiv drift, men også større konsekvenser ved nedetid i IT systemene. Fylkeskommunen har ikke bare et ansvar for sine egne IT systemer. Men er også en tilbyder av forskjellige IKT tjenester til befolkningen i fylket. Dette fordrer robuste IT løsninger. Befolkningen ønsker i stadig større grad å kommunisere med det offentlige ved hjelp av digitale selvbetjeningsløsninger. Kommunenes Sentralforbund (KS) vektlegger spesielt forholdet til innbyggerne med mål om stadig flere digitale tjenester og intern effektivisering. KS har laget følgende visjon for eKommune 2012: *"Norske kommuner og fylkeskommuner skal være blant de fremste i verden på elektronisk innbyggerdialog, digitale tjenester og effektiv e-forvaltning."* (*eKommune 2012,s.5*)

Siden 1990 har alle salige organisasjoner måttet ha en virksomhetsplan med overordnete mål. Mål- og resultatstyringssystem, som et instrumentelt system, bør ideelt sett være basert på mål som politikere formulerer, og disse målene skal igjen reflektere ønsker og behov i befolkningen. Politisk definerte mål skal så virkeliggjøres i en administrativ iverksettingsprosess. Christensen m.fl. (2004) omtaler offentlig sektor som «*multifunksjonelle. Dette innebærer at de skal ivareta delvis motstridende hensyn, som politisk styring, kontroll, representasjon og deltakelse fra berørte parter, medbestemmelse fra ansatte, lydhørhet overfor brukere, åpenhet, offentlighet og innsyn i beslutningsprosessene. Forutsigbarhet, likebehandling, upartiskhet, nøytralitet, tjenestekvalitet, faglig uavhengighet, politisk lojalitet og kostnadseffektivitet.» (*Christensen m.fl., 2004, s.18).

Offentlig sektor som fylkeskommunen har både et brukeroppdrag og et samfunnsoppdrag. De fleste arbeidsprosesser som utføres i fylkeskommunen er ledd i et tjenestetilbud til enten innbyggere, organisasjoner, næringsliv og ansatte. Mange av disse prosessene er, eller skal i så stor grad som mulig automatiseres. Tjenesteområder som henger sammen, vil automatisk kunne utveksle informasjon digitalt der taushetsplikt eller annen lov ikke er til hinder for dette. Fagsystem på ett tjenesteområde kan generere en aktivitet i fagsystemet på et annet tjenesteområde ved aktuelle hendelser.

En god nettside setter brukerens behov i sentrum, og organiserer informasjonen ut fra brukerbehovet. I tillegg skal den gi en god oversikt over informasjon og tjenester, samt gi mulighet til dialog og innsyn i for eksempel politiske saker. Bruk av sosiale medier er en effektiv måte å kommunisere på, blant annet fordi mottakeren kan få informasjonen direkte inn på sin profil. For fylkeskommunen kan sosiale medier være viktige kommunikasjons og beredskapskanaler. For eksempel ved krisesituasjoner kan det være behov for døgnkontinuerlig opplysninger til befolkingen.

2.5 Fylkeskommunens strategi og sikkerhetsstyring

Strategi for anvendelse av IKT med dette menes hvordan fylkeskommunen som virksomhet skal møte de utfordringene som kommer i form av nye ønsker og behov hos innbyggere. Med stadig strammere økonomiske rammer, er det stort fokus på effektivisering. Som oftest ligger de største gevinstene i digitalisering av tjenester og automatisering av disse der det er mulig. For å hente ut effektiviseringsgevinster ved IKT-satsninger er endringsvilje og organisasjonsutvikling en forutsetning for å lykkes.

Tradisjonelt sikkerhets- og beredskapsarbeid hos fylkeskommunen handler om tiltak for å forebygge og effektivt kunne håndtere hendelser og situasjoner som truer liv, helse, miljø. I den nyere tid er beredskapsarbeidet også blitt håndtering av trusler og terror da spesielt på skolesiden.

3 TEORI

Kapittelet er bygd opp med den hensikt å belyse forskjellige teorier knyttet til de fem forskjellige temaene som går igjen gjennom hele oppgaven.

3.1 Sikkerhetsstyring

3.1.1 Ledelse

Ledelse kan være å påvirke mennesker direkte, for eksempel gjennom samtaler, ulike former for ordrer og direktiver, eller gjennom å støtte og inspirere medarbeidere. Men ledelse er også å være sentral i utforming av mål. Jacobsen og Thorsvik (2007) skiller mellom følgende kulturelle nivåer i organisasjonen:

- *«Artefakter- synlige utrykk for kultur, men ikke alltid lett å tolke.*
- *Verdier og normer- høyere grad av bevissthet.*
- *Grunnleggende antagelser- tatt for gitt» (*Jacobsen og Thorsvik, 2007, s.123).

Disse tre nivåene er vesentlige for å forsterke samspillet, samordningen og samarbeidet mellom ledelse og de ansatte. Det er viktig at alle har en lik forståelse spesielt vil dette gjelde mål og strategi, hvor skal vi og hvordan skal vi komme dit. *«Organisasjoner er avhengig av sine omgivelser for å overleve. For å overleve må organisasjonens mål, strategi og struktur være tilpasset til omgivelsene.» (*Jacobsen og Thorsvik, 2007, s.189). Dette stemmer godt overens med hva fylkeskommunen har å forholde seg til både eksternt og internt.
For å nå sine mål og strategier, både internt og eksternt, er blant annet et godt arbeidsmiljø viktig. Godt arbeidsmiljø vil kunne bidra til et kollektivt forståelsesapparat og igjen gjensidig motivasjon. For å få til en god og sammensveiset gruppe medarbeidere, er motivere medarbeidere er et viktig virkemiddel. Jacobsen og Thorsvik (2007) viser til forskning av Fredrick Herzbergs angående trivsel på arbeidsplassen. *«Ansattes tilfredshet i arbeidet var knyttet til arbeidets karakter, mistrivsel i arbeidet var knyttet til arbeidsmiljøet.» (*Jacobsen og Thorsvik, 2007, s.226)

*«IKT-sikkerhet er først og fremst et virksomhetsansvar. Dette følger av ansvarsprinsippet, som innebærer at den som har et ansvar for en virksomhet under normale forhold, også har et ansvar ved en krisesituasjon. I praksis innebærer dette at primæransvaret for sikring av informasjonssystemer og nettverk ligger hos eieren. Samvirkeprinsippet stiller krav til at myndighet, virksomhet eller etat har et selvstendig ansvar for å sikre et best mulig samvirke med relevante aktører og virksomheter i arbeidet med forebygging, beredskap og krisehåndtering.» (*St.meld.nr.29, 2011-2012, s.106)

Fylkestinget kan selv bestemme at ledende administrative stillinger skal besettes på åremål. Slikt åremål skal være på minst seks år. Det kan være en utfordring for strategi og langtidsplanleggingen når ledelsen tilsettes på åremål istedenfor permanent tilsettelse. Dette er politisk bestemt og lovpålagt og gjelder i fylkeskommunens tilfelle.

(Ot.prp. nr. 96, 2005-2006)
Fylkeskommunen har et generelt og grunnleggende ansvar for å ivareta befolkningens tjenestetilbud innenfor sine geografiske områder, samt økt verdiskapning og bærekraftig utvikling av fylket. I det ligger det at de skal være opptatt av innbyggernes ve og vel. Det har hele tiden vært en klar forventning fra storting og regjering at dette blir ivaretatt. På bak grunn av dette må fylkeskommunene ta sikkerhets- og beredskapsmessige hensyn i mål og strategiplanleggingen. Fylkeskommunen har ikke noen konkret lovpålagt beredskapsplikt når det gjelder IKT sikkerhet innad i virksomheten. Det er heller ikke noen krav for revisjon av IKT sikkerhetsarbeidet i forhold til sentrale myndigheter. Desto viktigere er det at ledelsen har fokus på IKT sikkerhet, at dette er formidlet, ansvar plassert og forstått blant ansatte. Og at det regelmessig gjennomføres øvelser for best mulig å ivareta IKT dersom det skulle oppstå en uønsket hendelse.

I boken *Hvordan organisasjoner fungerer* Jacobsen og Thorsvik (2007) beskrives mennesketyper som er sosiale, flinke, pågående og arbeidsomme, kan være gode ledere. Dette er gode egenskaper som kan gi et sterkt engasjement og tillit hos de ansatte. Disse egenskapene bør alle ledere inneha, spesielt bør IT leder ha slike kvalifikasjoner og se på seg selv som en ambassadør for ledelsen og medarbeidere. Christensen m.fl.(2004) snakker om mellomleder som krysspress ovenfra og nedenfra. Med dette menes at det er helt avgjørende å skape forståelse, og god formidling for en beslutning fra ledelsen. Andre ganger vil være vedkomne være medarbeiderens talerør overfor ledelsen og ta opp saker som de har sterke meninger om. I posisjonen mellom «barken og veden» må IT leder trene og utvikle ferdigheter som kan fører til omdannelse fra motstand til medvirkning.

3.1.2 Sårbarhet i organisasjoner

Enhver organisasjon må balansere forholdet mellom produksjon og beskyttelse. Reason (1997) hevder at de produktive aspektene ved en organisasjon vanligvis er tydelige og godt kjent og forstått, men at organisasjonens beskyttelsesfunksjoner kan være av mer varierende grad og omfang og ofte mer underliggende. Det som til slutt avgjør forsvarsverkets funksjon er økonomi. Det vil si er det økonomi som bestemmer ulykkesrisikoen.

Noen forhold som kan føre til nedprioriteringer av IKT sikkerheten i virksomheten kan være, stram økonomi, liten vilje eller kompetanse fra ledelsen, endret kurs i virksomheten som for eksempel omorganisering og lignende. Dersom virksomheten skal spare penger ser man som oftest at det blir kuttet ned på forebyggende sikkerhetsarbeid. Årsaken kan være at virksomheten har vært skånet for kritiske hendelser og derfor blir blindet av trusselbildet. Det være seg både tilsiktede hendelser og utilsiktede hendelser. Ulempen med dette er svekket sikkerhetsstyring og dårlig forebyggelse av IKT beredskapsarbeid, som igjen fører til mindre robust og mer sårbar virksomhet.

Dette kommer kanskje av for liten bevissthet. Weick m.fl.(1999) har utviklet en teori om bevissthet (mindfulness) i organisasjoner. Årsaken til at noen organisasjoner behersker uønskede hendelser bedre enn andre er at de har et konstant fokus på dette. Mindfulness

dreier seg om oppdagelse av uventede hendelser som kan oppstå hvor som helst i organisasjonen og at dette er en form for dynamisk kompetanse som stadig er i utvikling, og som innrullerer nye erfaringer, bevissthet om at det utenkelige faktisk kan skje.

Uønskede hendelser, kriser eller kriselignende situasjoner vil aldri helt kunne unngås, men det er mulig å redusere sannsynligheten for og konsekvensen av uønskede hendelser gjennom et systematisk arbeid. For å få til dette må det forebyggende arbeidet ha prioritet. En målsetning bør være at virksomheten skal bli så robust som mulig. Dette vil igjen føre til mineralisering av risikoen for uønskede hendelser og for å kunne takle det som måtte oppstå best mulig. Klare del og langtidsmål kan oppnås ved systematisk arbeid og god styring. (Jan T. Bjørnsen, 2012) beskriver sikkerhetsstyring som sammensatte og forskjellige oppgaver, utfordringer vil være:

- *«Et administrativt, ikke teknisk aspekt som krever at det avsettes tid og ressurser til planlegging og organisering hos foretakets ledelse.*
- *Et operativt, teknisk aspekt som krever vilje og gjennomføringsevne samt forankring i ledelsen, slik at ressurser blir avsatt.*
- *Statiske og langsiktige teknologiske/forretningsmessige perspektiv for virksomheten.*
- *Dynamisk evne til hurtig omstilling og vilje til å ta i bruk ny teknologi og nye forretnings muligheter.»* (Jan T. Bjørnsen, 2012, s.65)

For at rådmann skal kunne fatte rett beslutninger, må det være en god samhandling og tett samarbeid med medarbeidere som har ansvar, vedlikehold og drift av IKT systemene. Avgjørende suksesskriterium for hvorvidt fylkeskommunen innehar et godt IKT sikkerhetsarbeid, er medarbeidernes evner å gi en tilbakemelding på vesentlige forhold som berører deres daglige sikkerhetsarbeid, og at ledelsen evner å fange opp denne tilbakemeldingen og forholder seg til dette.

I virksomheter som har god sikkerhetsstyring, og som samtidig klarer å engasjere, inkludere, involvere og kommunisere IKT sikkerhet og sikkerhetsarbeidet innad i virksomheten, vil man kunne stå bedre rustet til å håndtere en uønsket hendelse. Reason (1997) Har fokus på organisatoriske forhold og bakenforliggende årsaker er et sentralt element i Reasons modell for organisatoriske ulykker. Noe av det som kjennetegner organisatoriske ulykker er at de skjer sjelden. Rekkevidden av slike ulykker rammer utover organisasjonen og årsaken er kompleks og omfatter forskjellige nivåer i organisasjonen. Reason peker på organisasjons motstandsdyktighet eller sårbarhet. Han illustrerer dette gjennom begrepet sikkerhetsrommet. Med dette begrepet mener han at man kan plassere organisasjon når det gjelder den nåværende motstandsdyktighet eller sårbarhet. Videre mener han at en organisasjons plassering i sikkerhetsrommet blir bestemt av kvaliteten på organisasjonens forvarsbarrierer. Plasseringen i sikkerhetsrommet er ikke konstant, men er hele tiden i bevegelse. Reason mener det er tre forhold som påvirker en organisasjons plassering i sikkerhetsrommet; fokus på sikkerhet, kompetanse og bevissthet omkring sikkerhet.

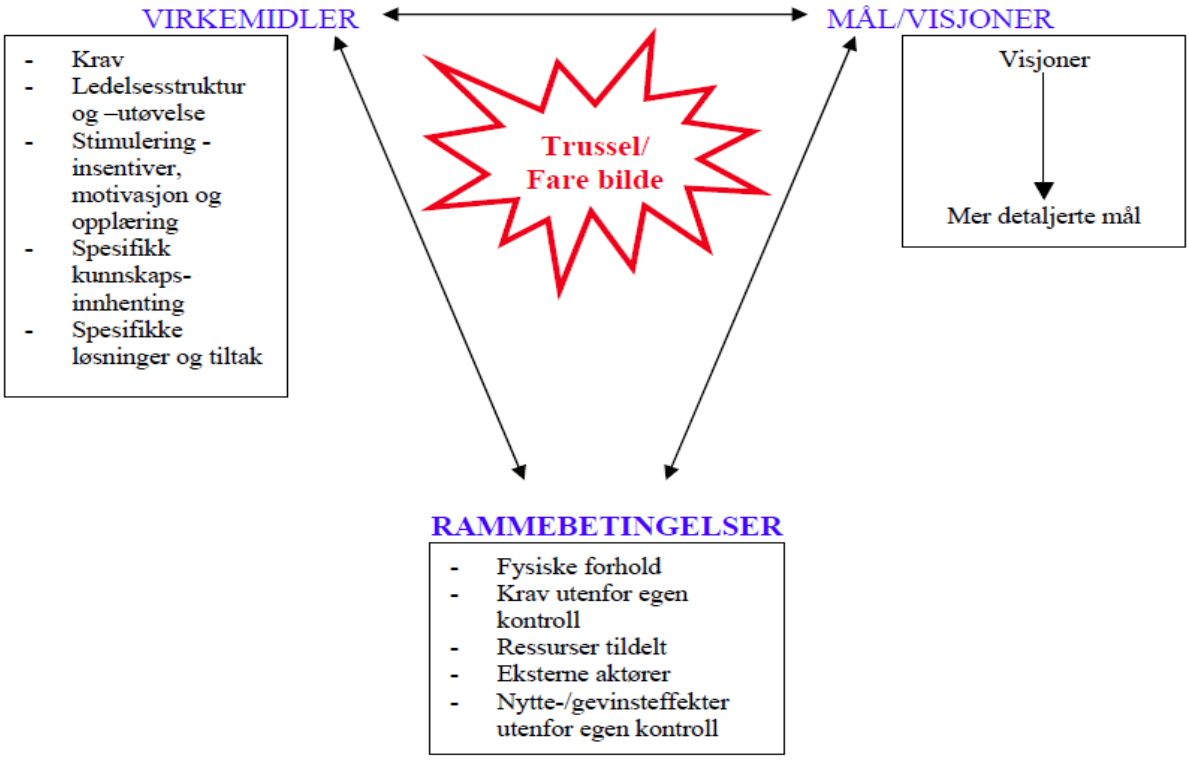
3.1.3 Strategi, mål og visjoner

Mål er en beskrivelse av en ønsket framtidig tilstand, er strategi en beskrivelse av hva man tenker å gjøre for å realisere målene. Strategien beskriver med andre ord «veien

mot målet».(Jacobsen og Thorsvik, 2007) mener det kan skilles mellom to ulike perspektiver på strategi. Det ene perspektivet kalles ofte for «ressursbasert» og er først og fremst knyttet til hvordan en organisasjon posisjonerer seg når det gjelder sine omgivelser. Det andre perspektivet kalles for «resultatbasert», og retter fokuset mer i mot interne forhold i organisasjonen, nærmere bestemt de trekk ved organisasjonen som gir den et fortrinn framfor andre organisasjoner.

Styring av IKT har styringsmessige konsekvenser for alle fylkeskommunale oppgaver. For å få til en god sikkerhetsstyring i fylkeskommunen er det viktig at den blir integrert i all strategi, planleggings- og prosjektarbeid. Sikkerhetsstyring må ikke være preget av skippertak, men være en kontinuerlig prosess. Derfor er det viktig at styringen må være tydelig, effektiv og ha god konsistens og at ansvars og oppgavedelingen for de enkelte er mottatt og forstått.

Aven m.fl.(2004) mener definisjonen av sikkerhetsstyring har to hovedelementer. Det ene er mål (visjoner) og det andre er tiltak (virkemidler). I tillegg kommer rammebetingelsene som mål og tiltak opererer innenfor. Mål eller visjonene kan være alt fra ansattes trivsel, til solid økonomi. For å nå målene eller visjonene må virksomheten benytte seg av forskjellige virkemidler.



Figur 3-1 *"Modell for sikkerhetsstyring"* (Aven m.fl., 2004, s.68)

Gjennom lov og instruksverk er fylkeskommunens hensikt og oppgaver definert. Delegasjonsreglementene beskriver hvordan fylkeskommunens makt og myndighetsutøvelse er fordelt i det politiske og administrative apparatet.
En viktig faktor i fylkeskommunen er å utvikle og vedlikeholde sikkerhetsmålene ved å sette seg visjoner, kortsiktige og langsiktige mål. Som er mulige å oppnå under rammebetingelsene som fylkeskommunen må forholde seg til. Disse målene vil være

vesentlig for den IKT sikkerhetsforståelsen som dannes.

3.1.4 Virkemidler

Aven m.fl.(2004) mener det er veldig mange måter å styre sikkerheten på, de kan for eksempel grupperes slik:

1. Krav – lover, forskrifter, regler og andre krav
Kravene kan være stilt av myndighetene, men kan også ha interne krav. Slike interne krav er ofte et viktig virkemiddel for å nå fastsatte mål. .

2. Ledelsesstruktur og – utøvelse
Utarbeidelse av mål og visjoner og utforming av løsningsforslag og tiltak

3. Stimulering – insentiver, motivasjon og opplæring
Igangsetting av tiltak for å få ansatte til å bevege seg i en spesiell retning for eksempel til å arbeide for å øke sikkerheten. Slik stimulering kan være rettet mot hele virksomheten eller enkeltpersoner.

4. Spesifikk kunnskapsinnhenting
Omhandler tiltak som er rettet mot hele virksomheten eller enkeltpersoner, for å få disse til å bevege seg i en spesiell retning.

5. Spesifikke løsninger og tiltak – tekniske, organisatoriske og operasjonelle tiltak
«Utarbeidelse av løsningsforslag handler om: ressurser som er nødvendige, hva som skal gjøres, og hvilke verdier som er prioritert.» (Aven m.fl., 2004, s.78)

3.1.5 Rammebetingelser

Aven mener rammebetingelser må oppfattes som relevante forhold for sikkerhetsstyringen, og er blant annet avhengig av disponible ressurser og situasjonen. *«Det som er rammebetingelser for noen kan være virkemidler for andre.»* (Aven m.fl., 2004, s.69) Skille mellom rammebetingelser og virkemidler kan i noen sammenhenger gå over i hverandre. Det som er avgjørende for å oppfatte om det er rammebetingelse eller virkemiddel er på hvilket nivå en opererer på og hvilke resurser som er til rådighet. Eksempel på rammebetingelser kan være: fysiske forhold, krav utenfor egen kontroll, tildelte ressurser og eksterne aktører.

3.2 Beredskap

Begrepet beredskap er definert som planlegging og forberedelser av tiltak for å begrense eller håndtere kriser eller andre uønskede hendelser på best mulig måte.
(NOU 2000:24, NOU 2006:6) Hensikten med beredskapsplanlegging er å planlegge strategier for uventede avbrudd, samt å beskytte kritiske prosesser mot negative konsekvenser ved feil eller uhell.
Aven m.fl.(2004) deler sikkerhet og beredskapsarbeidet i to hovedretninger:

• I den første retningen behandles spørsmål om sikkerhet og beredskap implisitt. I en slik retning er det ingen som har sikkerhet som sin hovedoppgave, sikkerhet og beredskapsarbeidet blir behandlet av personer som i utgangspunktet har andre oppgaver. Dette kan føre til at arbeidet med sikkerhet blir fragmentert og mangler helhetstenkning. Måten er derimot lite ressurskrevende.

• Den andre retningen behandles spørsmål om sikkerhet og beredskap eksplisitt. I en slik retning har utnevnt personell i en planleggingsgruppe ansvaret for det som angår sikkerhet og beredskap. Sikkerhet blir da en prosess på linje med andre prosesser og blir en mer integrert del av planleggingen. De som arbeider med sikkerhet og beredskap er ansvarlige for utvikling av sikkerhetssystemer og bevisstgjørelse av IKT sikkerhet blant medarbeidere.

IKT-beredskap er en meget vesentlig del av sikkerhetsplanleggingen, og krever mye arbeid på alle nivåer i sikkerhetsstyringen. IKT-beredskapsplaner må fokusere på hvordan virksomheten skal videreføre sine virksomhetskritiske prosesser dersom de skulle bli rammet av en uønsket hendelse som setter store deler av virksomheten ut av spill. Man kan si det er to forskjellige IKT sikringstiltak i denne sammenheng, teknisk og ikke teknisk.

- Teknisk - sikring aktivisering og beskyttelse av utstyr. Eksempler på dette er backup, logger, virus kontroll, brannmur ol.
- Ikke teknisk - sikring som for eksempel gode retningslinjer for bruk av IKT systemer, god beredskap/ kriseplan, gjennomførte og evaluerte øvelser,

Disse sikringstiltakene til sammen vil dette kunne hindre at en tilsynelatende liten uheldig hendelse blir til en stor krise.

3.2.1 Risiko

Begrepet *risiko* kommer av det Italienske ordet «risicare» som betyr å våge. (Bernstein 1996). (Aven 2007, s. 41) definerer risiko som «*en kombinasjon av mulige konsekvenser (utfall) og tilhørende usikkerhet*».
En annen definisjon er: *«Risiko er en funksjon av sannsynligheten for mulige uønskede hendelser og konsekvensene av disse. Risiko uttrykker fare for tap av viktige verdier som følge av uønskede hendelser. Viktige verdier kan for eksempel være liv og helse, miljø, økonomi og gjennomføring av kritiske samfunnstjenester.*» (NOU 2000:24, s.21)

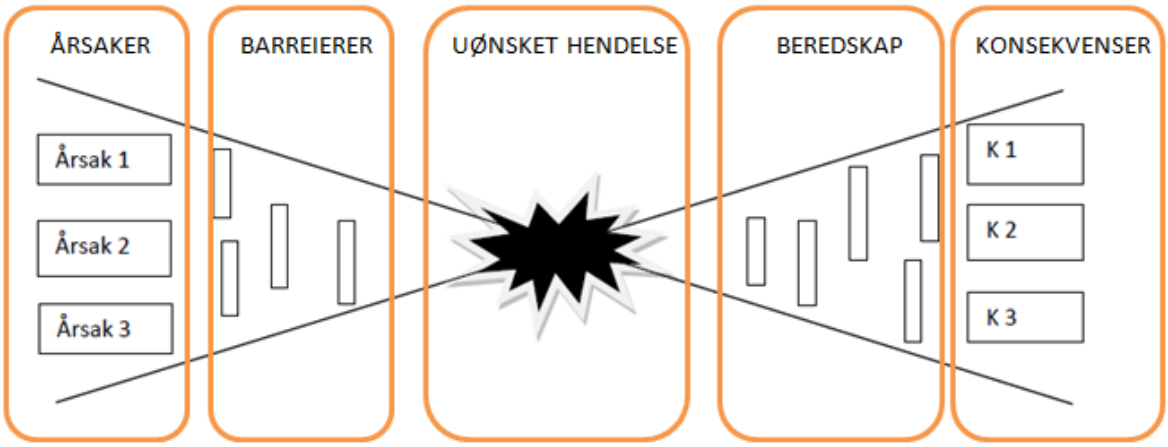
Det er viktig å ha en forståelse og kjennskap til hva som kan være risikofylt og hva som påvirker risiko og sårbarhetene som finnes i fylkeskommunen. Og hvilke konsekvenser det kan ha om IKT systemene brister. Ved konstant å overvåke og ta signaler både internt og eksternt i virksomheten kan man vurdere risiko og sette inn tiltak. Trusselbildet vil ha stor betydning når det gjelder hva som er ansett som risiko. Det være seg utilsiktede hendelser som, for eksempel naturkatastrofer ol. Eller tilsiktede hendelser som, tyveri og hærverk ol.

Reason (1997) skriver om at lengre perioder uten uønskede hendelser i en virksomhet vil føre til svekket fokus på sikkerhetsarbeidet. Dette fordi fokuset blir sterkere rettet mot produksjonsmålene. Ledelsen og de ansatte har ofte lett for å glemme frykten for det som hender sjeldent eller aldri har hendt, men som allikevel er en risiko. Effekten av dette kan føre til interessen, og nødvendige øvelser for å bevare eksisterende sikkerhetsnivå blir borte.

3.2.2 Risiko og sårbarhetsanalyser

Risiko og sårbarhetsanalyser (ROS)omfatter en systematisk identifisering og kategorisering av risiko og sårbarhet (Aven m.fl. 2004). Analysene er viktige som beslutningsstøtteverktøy i forhold til sikkerhetsstyringen. Både for å unngå tap, men og for en best mulig prioritering av ressursene dersom uønsket hendelse skulle inntreffe. Ved hjelp av analysene vil man forsøke å kartlegge hvilke hendelser som kan forårsake databortfall. For eksempel en uønsket hendelse som brann i hoveddatarom sentralt i fylkeskommunen. En slik brann ville kunne sette en hel fylkeskommune ut av spill. Konsekvensene kunne bli enorme, alt av oppgaver og tjenester kunne bli berørt.

Figur 3-1 «Bow-tie-diagram» illustrerer årsak-konsekvens kjede. På diagrammets venstre side vil årsakene og de ulike barrierer som skal forhindre uønsket hendelsen i å inntreffe. Disse barrierene blir omtalt som sannsynlighetsreduserende eller forebyggende. På diagrammets høyre side er ulike beredskapstiltak eller omtalt som konsekvensreduserende barrierer, som skal begrense eller hindre at hendelsen får alvorlige konsekvenser.



Figur 3-1 «Bow-tie-diagram» (Aven, 2008, s. 46) figuren er en forenklet utgave.

Eksempel på momenter som kan inngå i et bow-tie-diagram

ÅRSAK	BARRIERE	HENDELSE	BEREDSKAP	KONSEKVENS
Strømbrudd	Nødaggregat virker ikke.	Server går ned	Reserveserver, feil i oppsett.	Data mistet.

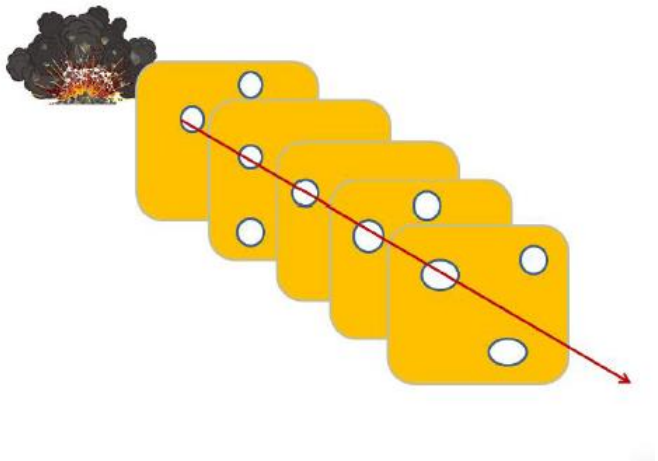
3.2.3 Risikostyring

Formålet med risikostyringen er å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap. Reason (1997) legger vekt på å identifisere prinsipper som kan brukes i virksomheter der en kan oppleve uønskede hendelser. Hans teorier og modeller er ment å kunne benyttes i alle typer virksomheter.

Reason (1997) skiller mellom to typer barrierer som kan beskytte en virksomhet mot ulike hendelser og tap. Den ene typen er harde barrierer som for eksempel fysiske

barrierer og sikkerhetsutstyr. Den andre typen barrierer, myke barrierer, som for eksempel regler og rutiner, opplæring og øvelser. Det er den siste typen barrierer som er gjeldende for IKT beredskap.
«Defences in depth», forsvar i dybden, betyr at det etablereres flere barrierer mot samme hendelsesforløp for å oppnå tilstrekkelig beskyttelse. Hver barriere er designet for å tre i kraft om den foregående bryter sammen. Reason er av den oppfatning at ulykker langt på vei kan unngås gjennom godt forebyggende arbeid ved bruk av forsvarsverk i flere lag og redundante løsninger. Forsvarsverket kan advare og alarmere når faren er nær eller gjenopprette et system til en sikker tilstand etter en hendelse. Det kan også sikre og eliminere farer om de slipper forbi en barriere, og dersom dette også mislykkes kan et forsvarsverk fungere som redning ved at de gir en fluktvei.

Sveitserostmodellen illustrerer tankegangen bak forsvarsverk i dybden. Modellen har fått sitt navn fordi et forsvarsverk kan tenkes oppbygd som lag på lag med sveitserostskiver. I hvert lag er det noen hull, men til sammen vil de danne et tett forsvar. På den måten kan man forhindre at en enkelt feil medfører en ulykke. Hver barriere har ulik karakter og virker på forskjellig måte. Reason (1997) viser i sin modell at sikkerhetsbarrierer som et forsvar mot svikt, ulykke eller katastrofe, kan ha svakheter som lett trenges gjennom.



Figur 3-2: «Sveitserost-modellen» av Reason (1997)

Barrierer brukes både for å redusere sannsynlighet for uønskede hendelser og for å eliminere eller begrense konsekvenser av slike. En helt klar målsetting bør være å forebygge at en uønsket hendelse skal skje. Både valg av tekniske løsninger med gode sikkerhetsegenskaper og valg av godt gjennom arbeidet ROS analyse, samt godt planverk er barrierer som inngår i tiltak for å forebygge uønskede hendelser.

Beredskapsplan er en planverk utarbeidet på bakgrunn av funn i ROS. Den bør inneholde alle elementer for å opprettholde situasjonen så normal som mulig. Beredskapsplanen er et viktig verktøy i en krise situasjon. En beredskapsplan er et levende dokument som må testes og evalueres med jevne mellomrom. IT Medarbeiderne vil være på det operative nivået, det er de som skal bruke IKT beredskapsplaner og det er som oftest de som har en formening om hvilken sikkerhets tilstand som rår i virksomheten. Det er som oftest de som innehar kompetanse og har en kultur for å tenke sikkerhet forhold til IT. Det er disse IT medarbeiderne som kan komme med gode innspill til ROS analyser som igjen er bakgrunn for beredskapsplan.

Det kan være at planen som resultat ikke nødvendigvis får noen verdi. Det betyr ikke at prosessen ved å lage en plan har vært bortkastet. Den har likevel resultert i synergier som ikke vises i planen, men i bevisstheten blant de som har deltatt i prosessen.

3.2.4 Øvelse og læring

Øvelser skal gi hele eller deler av virksomheten kompetanse og trygghet til å håndtere unormale hendelser og kriser. Det er viktig å øve ansatte, da med tanke på hvordan hele virksomheten ville håndtert en uønsket hendelse. Dette vil igjen bidra til at man kan møte en uønsket hendelse best mulig forberedt. Planlegging i forkant og evaluering i etterkant av en øvelse styrker i tillegg samarbeidet og kunnskapen til de som deltar. Øvelser skal være en naturlig del av alle etaters, organisasjoners og bedrifter virksomhet. Direktør i DSB Jon A. Lea sier det slik: *«Øvelser har liten verdi dersom man ikke nyttegjør seg de erfaringene som evalueringer i ettertid gir, hensikten med øvelse er å lære.»* (*DSB, Samfunnssikkerhet, Nummer 03. september 2012,s.26*).

For at en organisasjon skal være i stand til å lære, forutsettes det at organisasjonen består av lærende individ. Dette er en nødvendig forutsetning ettersom arbeidsoppgavene utføres av individer i organisasjonen. Individene må endre sine oppfatninger av arbeidet som skal utføres, eller endre måten de utfører arbeidet på. Det er derfor ikke slik at den individuelle læring i seg selv skaper endringer på organisasjonsnivå. Organisasjoner endres i samspillet mellom aktørene, både mellom individ og grupper (Levin og Klev, 2009).

Jacobsen og Thorsvik (2007) skriver om lærende organisasjoner og systemtenkning. En suksessfaktor vil blant annet være langsiktig strategi, og satsing på praktisk problemløsning for å oppnå en kontinuerlig forbedring i alt arbeid som utføres. Dette er en utfordring i offentlig sektor. Med et politisk styrende organ og ledelse som skiftes ut med noen års mellomrom. I offentlig sektor vil derfor alltid være en stor utfordring å få gjennomført langsiktige og strategiske strategier kanskje spesielt når det gjelder IKT sikkerhet og beredskap, spesielt om trusselnivået er vurdert som lavt.

Fimreite, m.f.(2011) skriver om betydningen av øvelser, at øvelser kan nyttiggjøres både til forebygging og beredskap. De viser til forskjellige typer øvelser, deriblant skrivebordøvelse. Denne øvelsetypen omfatter som regel ledelsen og nøkkelpersoner og er lite ressurskrevende, tidsbesparende og ansvarsbevisst. Å arrangere en slik type øvelse vil øke bevisstheten.

4 METODE

I dette kapittelet vil jeg presentere mitt valg av metode for oppgaven, og hvordan den innsamlede data er blitt behandlet, i den hensikt å gi svar på studiens problemstilling. Kapittelet er bygd opp slik: valg av metode for oppgaven, litt om hvilken datainnsamling som er benyttet, valg av respondenter, beskrivelse av framgangsmåte for gjennomføring av spørreundersøkelsen. Avslutningsvis litt om validiteten og reliabiliteten i oppgaven.

4.1 Utforming og design

Forskningsdesign er bindeleddet mellom de spørsmål man ønsker å få svar på, og innhenting av data som skal belyse den aktuelle problemstillingen. Forskingsarbeid kan foretas på flere måter. Det metodiske valget er avhengig av hvilke data man ønsker å samle inn, og hvilken fremgangsmåte som er relevant når det gjelder forskingsarbeidet som blir gjort.

IKT sikkerhet er mitt fagområde og fylkeskommunen er og har vært min arbeidsgiver over flere år. Jeg mener å kunne si at ved å kjenne fagområde godt er det flere fordeler enn svakheter. Føler selv at min bakgrunn har bidratt til å styrke oppgaven med tanke på forhold som blant annet kjennskap til virksomhetsstyring og struktur i fylkeskommunen, og IKT sikkerhetsarbeidet i min fylkeskommune. Min erfaring fra IKT sikkerhet i fylkeskommunal virksomhet, vil naturlig nok ha innvirkning på gjennomføringen av denne oppgaven. Minus må sies å være mulige fordommer som har preget forskningsprosessen, det vil si at jeg har hatt antakelser om hvordan ”verden” ser ut, og kan ha en forutinntatthet med tanke på oppgavens funn og konklusjoner. Oppgavens relevans er en følge av dette. Spesielt ved formulering av problemstillingen og utarbeidelse av spørreundersøkelsen var det en stor fordel å kjenne fagområdet.

Det er to tilnærmingsperspektiver innenfor forskning, kvalitative og kvantitative design. De to metodene representerer hvert sitt kunnskapsperspektiv. Avgjørende for metodevalget er hva man ønsker å vite. Kort fortalt sier kvalitativ metode noe om opplevelse rent følelsesmessig og kvantitative sier noe om hvor mange (tall) som kan behandles videre ved hjelp av statistiske teknikker. (Jacobsen, 2000).
I min oppgave går vegen fra teori til empiri via en kvantitativ tilnærming. Som en av flere metoder for oppgavens datagrunnlag er det tatt utgangspunkt i kvantitativ spørreundersøkelse. Denne metoden er å foretrekke når det ikke er snakk om en konkret tilstandsrapport. Noe som passer godt til min oppgave, siden det er «nå» tilstanden jeg ønsker å kartlegge.

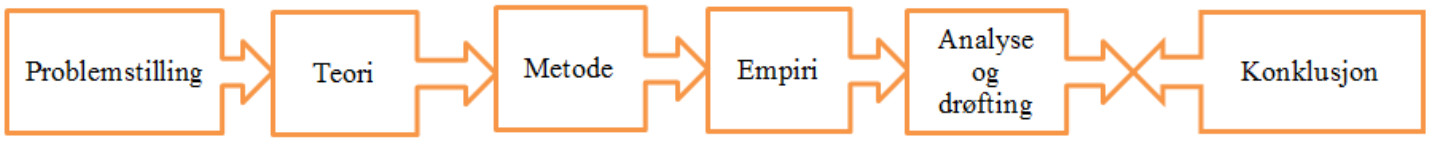
Fordelen med kvantitativ metode kan være at spørsmålene er fastlagt før datainnsamlingen begynner, samtidig som det er forhånds bestemt hvilke utvalgte aspekter som skal undersøkes. Andre fordeler kan være at man ønsker å vite noe om flere enheter spredt over et stort geografisk område, lavt kostnadsnivå og tidsbesparelse. Ulempen i kvantitativ metode kan være ikke fysisk og psykisk nærværelse av

respondentene som igjen kan føre til bedre besvarelse. Respondentene har ingen mulighet for å gå i dybden av spørsmålene å få frem mangfold og nyanser i sine svar.

Problemstillingen og teorivalget som er foretatt vil legge føringer for strategien, og hvilket datamateriale som kreves for å besvare problemstillingen. I denne oppgaven er de kvantitative dataene fremstilt i form av en spørreundersøkelse. Det ble sendt ut et spørreskjema til personer i sentrale stillinger med tilknytning til fagområdet. Målet var å få innsikt i de enkeltes holdninger og tanker rundt temaet og hvordan respondentene ser sin egen og hverandres rolle i IKT arbeidet.

Utviklingen av spørsmålene startet tidlig, bakgrunnen for at jeg interessert i tematikken er at dette er mitt fagfelt. Jeg hadde mange tanker og notater fra tidligere som ble til et godt hjelpemiddel i utformingen av spørreskjema. Svært mye av det arbeid som er gjort med denne oppgaven er basert på egen erfaring og observasjoner.

Selve utformingen av oppgaven vil se slik ut:



Figur 4 -1 utformingen av oppgaven

Kapittel1-Problemstilling, kapittel 3-Teori og perspektiv for analyse, kapittel 4-Metode, kapittel 5- Empiri, kapittel 6- Drøfting og tilslutt i kapittel 7-Konklusjon.

4.2 Utvalg og respondenter

Jacobsen (2000) betegner et utvalg som undergruppe av populasjonen, utvalg i denne sammenheng er en mindre gruppe som trekkes ut fra den teoretiske populasjonen, for så å gjøre en konkret empirisk undersøkelse.

Det er tre valgte fylkeskommuner som har omtrent samme antall innbyggere, men er geografisk spredt. I alle fylkene er både reiseliv og turisme en viktig ressurs for fylket. Naturlig nok vil primærnæringen i fylkeskommunene være varierende, årsaken er geografisk spredning. To av fylkene er inndelt i omtrent like mange kommuner. De er også ganske like i forhold til areal. Det siste fylket har litt færre kommuner. Alle fylkeskommunene har cirka like mange ansatte. Samt at de har ansvar for omtrent like mange videregående skoler med ganske likt elevtall. De har også omtrent like mange tannhelseklinikker å serve og vedlikeholde. Det var viktig for meg at de fylkeskommunene jeg skulle ha besvarelser fra, hadde omtrent likt innbygger tall og helst at de var geografisk spredt, som igjen vil gjøre analysen mer interessant. Ut i fra dette grunnlaget vil besvarelsene kunne sammenstilles.

Videre skiller Jacobsen (2000) mellom informanter og respondenter, informanter representer ikke gruppen, men har god kjennskap til gruppen. Respondenter er personer

som har direkte kjennskap til fenomenet, og representanter for gruppen som skal undersøkes. Alle mine besvarelser på spørreundersøkelsen er gitt av personer som har kjennskap til fenomenet.
Problemstillingen har lagt føringer for hva slags type respondenter det var ønskelig å kontakte. Det var viktig at stillingsgrupperingene går vertikalt i organisasjonen, ved å velge respondenter med forskjellig kompetanse og stilling blir bildet så nyansert som mulig. Det var ti personer som sa seg villig til å være med på undersøkelsen, to rådmenn, tre IT ledere og fem IT medarbeidere. Bidrag fra alle respondentene, hver på sin måte er verdifullt og betydningsfullt for å belyse oppgavens problemstilling.
Etter min mening er respondenter som innehar disse stillingene å betrakte som nøkkelrepresentanter for undersøkelsen. På bakgrunn av at fylkeskommunen er samme type virksomhet hvor som helst i landet, har også respondentene omtrent de samme oppgaver, utfordringer og problemer. Valget av respondenter ble gjennomført med tanke på å få best mulig data relatert til problemstillingene.

4.2.1 Respondenter:

Rådmann
Rådmann har det daglige ansvaret for fylkeskommunens virksomhet, og har som hovedoppgave å sikre en god samhandling og koordinering av arbeidet mellom fylkesrådet og administrasjonen. Som fylkeskommunens administrative leder har rådmann har det øverste ansvaret for sikkerheten, sammen med ledelsen iverksetter rådmannen strategier, målsettinger og visjoner vedrørende sikkerhet i fylkeskommunen. Dette arbeidet går igjen ut hos den enkelte mellomleder og andre medarbeidere, som gjennom sine daglige gjøremål og arbeidsrutiner skal praktisere IKT sikkerhet. For at rådmann med ledelsen kan gjøre sitt arbeid er de avhengig av tilbakemeldinger eller informasjon andre vegen, det vil si fra ansatt til ledelsen.

IT leder
IT leder er leder for fylkeskommunens IT avdeling eller enhet, og dermed den personen som har det fulle og hele ansvaret for IT sikkerhet i hele fylkeskommunen. Vedkomne er mellomleddet fra rådmann til IT medarbeideren, og har en faglig IT kunnskap som rådmannen ikke har. IT handler ofte om planlegging og raske omstillinger, og IT lederen opplever ofte å være i en sentral beslutnings og påvirkningsposisjon, eller føle seg «mellom barken og veden». Barken er forventninger og krav fra rådmann og ledelsen i fylkeskommunen. Veden er de ansatte og deres behov. Ofte blir arbeidshverdagen delt mellom jobben som fagperson i kombinasjon med lederjobben. Møteledelse, teambygging, målstyring, medarbeiderutvikling, konflikthåndtering, resultat- og økonomioppfølging er noen av de mange arbeidsoppgaver IT lederen står overfor. Om det skulle oppstå en krisesituasjon blir plassen mellom barken og veden redusert til null. IT lederen har det i prinsippet vanskeligere enn rådmann ved ledelsen. Dette fordi IT lederen må ta hensyn til hva som blir krevd fra ledelsen, samtidig må IT lederen ivareta sine ansatte slik at de yter best mulig.

IT medarbeider
IT medarbeideren er underlagt IT lederen og arbeider i IT avdelingen eller enheten. Det er disse menneskene som har det daglige arbeidet med, drift av IT utstyr som for eksempel servere, nettverksutstyr, brannmurer og annet utstyr. Andre arbeidsoppgaver

er utvikling av systemer og løsninger knyttet til drift, overvåking, samt etablering av rutiner og dokumentasjon. De fleste fylkeskommunene drifter og vedlikeholder det meste av sine egne systemer. Den spesialkompetansen de ikke innehar selv blir ofte kjøpt av eksterne konsulenter. Dersom det for eksempel skjer en uønsket hendelse med langvarig bort fall av data, vil IT medarbeideren bli sterkt involvert for raskest mulig å få IT systemene i gang igjen. Forøvrig kan nevnes at respondentene er fordelt på alle tre fylkeskommunene.

4.3 Data innsamling

Data innsamlingen har bestått av kvantitative metode i form av spørreskjema, dokumentstudier og litratursøk. Dette vil jeg igjen bruke som kildegrunnlag for min empiriske fremstilling og i drøftingskapittelet.

4.3.1 Dokumentstudier

Et viktig valg ved bruk av dokumentanalyse er utvalget av dokumenter og troverdigheten til disse (Jacobsen, 2000). I tillegg til en kvantitativ spørreundersøkelse har jeg lagt til grunn studier av Mørketallundersøkelsen™ 2012 som er gjennomført Næringslivets Sikkerhetsråd (NSR) gjennom Datakrimutvalget.
Fra TNS Gallup som har gjennomført selve undersøkelsen, har jeg fått oversendt en fil over alle besvarelser fra offentlig sektor. På bakgrunn av at det er bare tallmaterialet som er blitt oversendt, er anonymiteten blitt ivaretatt. Besvarelsene fra Mørketallundersøkelsen™ 2012 vil bli brukt som et «bakteppe» i min analyse. Med bakteppe menes at mange av funnene i undersøkelsen vil bli sett i lys av funn fra min spørreundersøkelse.

4.3.2 Litteraturstudiet

Mye av mitt daglige virke er å følge med på hva som skjer innenfor trender og utvikling av IKT. Opp gjennom tiden har jeg samlet mye relevant data, innsamlingen har blant annet foregått på internett, kurs og seminarer. Litteratur fra stortingsmeldinger, veiledere, statistikker, undersøkelser, forskrifter, lover og oppslag i media er benyttet. Flere av disse dokumentene brukes for å oppnå bedre kjennskap til både fagfeltet og hva som rører seg i «IKT verden». Det har vært helt naturlig å benytte en del av denne informasjon til min problemstilling. Litteraturstudiet er hovedsakelig gjort rundt tema IKT- sikkerhet, beredskap og risiko.

4.3.3 Spørreundersøkelsen

Etter en rekke alternativer til utformingen av spørsmålene ble det endelige valget presentert for veileder. Formuleringen av spørsmålene ble revidert, diskutert og evaluert i samråd med veileder. Med bakgrunn i denne evalueringen ble det endelige

spørreskjemaet utviklet. To kolleger, to pedagoger og en utenforstående til tematikken sa seg villig til å være en pilotgruppe for besvarelse av spørreskjemaene. De gav få, men gode innspill på uklare deler ved spørsmålene. Dette ble tatt med i utformingen av det endelige skjemaet.

Valg av utsendelse av spørreundersøkelse ble Questback(web basert verktøy for spørreundersøkelser og -analyser) valgt. Noen av fordelene ved Questback var at det var, gratis for studenter, enkelt å legge inn spørsmålene, gode rapport muligheter, og purremulighet til respondenter som ikke svarte på første henvendelse. Når alle spørsmålene var ferdig utformet og lagt inn i Questback. Testet pilotgruppen ut funksjonalitet og tid på besvarelse i alle testene kom man fram til ca. 15 min. Tilbakemeldingene var kort oppsummert et enkelt og veldig brukervennlig verktøy. Ved hjelp av en distribusjonsliste kunne alle respondentene nås effektivt. Ved å benytte Questback kunne spørreundersøkelsen nåes fra internett, en stor fordel med dette var at respondentene kunne da ta undersøkelsen når det passet best. Om respondenten avslutt halvveis, hadde vedkomne muligheten til å fortsette fra samme sted hvor man avsluttet på et senere tidspunkt. I tillegg kunne man gå både frem og tilbake i skjemaet. Det var en forutsetning at alle spørsmålene måtte besvares for å komme videre i undersøkelsen. Hvis respondenten valgte å la være å svare på hele undersøkelsen, ville besvarelsen heller ikke komme med i datasettet.

Spørreskjemaet var anonymt i forhold til respondenten og fylkeskommunen, fra tidligere forskning har det vist seg at ved å anonymisere respondentene er det lettere å få frem ærlige og oppriktige svar. Dette var årsaken til at jeg valgte å anonymisere respondentene. For oppgavens problemstilling har det heller ingen betydning å vite hvilken fylkeskommune som har, eller ikke har god IKT sikkerhet og beredskap.
For å avdekke eller måle holdninger blant respondenten bli som oftest et sett med påstander utformet, dette kalles rangordnede spørsmål. (Jacobsen, 2000). Spørsmålene var formet som påstander. De fleste påstandene var positivt vinklet, men noen var negativt vinklet, for å oppfordre respondenten til å lese utsagnet nøye.
Spørreskjemaet var delt inn i fem forskjellige temaer og er som følger:

- Interne IKT lover og regler: spørsmål som omhandler interne IKT lover og regler, hvordan dette blir overholdt og kvalitetssikret.
- Sikkerhetsstyring: spørsmål som omhandler sikkerhetsstyring i forhold til IKT sikkerhet og beredskap, hvordan dette blir kommunisert og hvilket fokus temaet har.
- Risiko og sårbarhetsanalyser (ROS): spørsmål som omhandler risiko og sårbarhetsanalyser (ROS).
- IKT Beredskapsarbeid: spørsmål som omhandler i hvilken grad ROS, ansvarsfordeling og handlingsplaner har påvirkning i beredskapsarbeidet.
- IKT øvelse: ble avdekket ved spørsmål som omhandler hvordan øvelse og læring blir ivaretatt.

Undersøkelsen inneholdt totalt 38 spørsmål, av disse var det 27 spørsmål, som hadde begrensede svaralternativer (helt uenig, nokså uenig, ikke uenig eller enig, noe enig og helt enig). I tillegg til de 27 spørsmålene var det 6 åpne spørsmål hvor respondenten selv måtte taste inn svaret, de var plassert slik at etter hvert tema var det et åpent spørsmål («boks») som oppfordret til eventuelle kommentarer eller tilbakemeldinger. Siste «boksen» nederst på skjemaet, var til andre kommentarer i forhold til IKT

sikkerhet og beredskapsarbeid i fylkeskommunen. Hver av «boksene» kunne inneholde 400 tegn. Hensikten med de åpne spørsmålene var å få fram momenter som ikke kom fram i de stilte spørsmålene. I tillegg var det 5 innledende spørsmål som omhandlet personalia.
Formålet med spørreundersøkelsen var å få best mulig data, slik at jeg kunne gjøre en grundig og god analyse, for så igjen besvare oppgavens problemstilling best mulig.

4.3.3.1 Fremgangsmåte

Før jeg begynte på selve oppgaven, utarbeidet jeg en grovskisse til spørsmål, som igjen omhandlet de fem forskjellige temaene i oppgaven. Etter å ha fått godkjent problemstilling fra Universitetet i Stavanger, og endelig kommet frem til de ferdige spørsmålene slik de framstilles i oppgaven, ble det gjort en henvendelse til forskjellige fylkeskommuner ved IT leder. Vedkomne ble kontaktet per telefon, og informert om spørreundersøkelsen og masteroppgavens hensikt. Dersom vedkomne var interessert i å være med, ble det sendt en mail med den samme informasjonen og ønske at de svarte på mailen for så igjen sende dem linken til spørreundersøkelsen. Den samme henvendelse ble gitt til rådmann dersom IT leder var interessert i å være med i undersøkelsen. I tillegg ble IT leder ble bedt om å informere alle ansatte på IT avdelingen, og svare på informasjonsmailen med e-postadressene til alle medarbeiderne slik at deres e-postadresser kunne legges inn i Questback. Dette var den enkleste måten å få e-postadressen til ansatte på IT avdelingen, slik at de kunne få tilsendt informasjon og link for besvarelse av undersøkelsen.

Det skal sies at det ble gjort flere forsøk før jeg fikk noen respondenter til å være med. To aktuelle IT ledere takket nei, de mente at dette ikke var noe for dem. En tredje IT leder takket ja, men ga ingen tilbakemelding, med e-postadresser til medarbeidere, dermed ble ikke sendt noe informasjon til andre i denne fylkeskommunen. Som sagt var det ikke alltid lett å få tak i respondentene, som regel ble det mange telefoner uten svar. Derfor ble det i to tilfeller sendt informasjonsmail til rådmann hvor vedkomne ble gjort oppmerksom på at leder for IT avdelingen stilte seg positiv til spørreundersøkelsen.

Spørreundersøkelsen var basert på frivillighet, respondentene fikk en god informasjon om undersøkelsens hensikt og hvordan resultatene skulle håndteres og brukes. Tidsbruken på besvarelse av spørsmålene ble oppgitt til ca.15 min. Det ble totalt utlevert tjueni undersøkelser, dato for utsendelse var den 24. april 2013 og fram til 6.mai 2013 ble det sendt ut purringer seks ganger til (11,15,1,1,1 og 20 mottakere). Informasjonsbrev er lagt ved som vedlegg 1 og spørreundersøkelsen kan i sin helhet leses i vedlegg 2.

4.4 Validitet og reliabilitet

Jacobsen (2000) mener undersøkelse kan være en metode for å samle inn empiri, og den bør tilfredsstille to krav:

- Gyldig og relevant (valid)
- Pålitelig og troverdig (reliabel)

4.4.1 Validitet

Validitet uttrykker gyldighet og relevans (måler det man har tenkt å måle).(Jacobsen, 2000) validiteten i spørreundersøkelsen avhenger av kvaliteten av de spørsmål som ble stilt, det vil si relevansen til teorien i oppgaven og forståelse av mine spørsmål. Kunnskap og stillingsperspektivet kan derfor medføre en viss risiko for feilkilder som skyldes at respondenten enten misforstår spørsmålene eller ikke kjenner til hvordan IKT sikkerhet og beredskap er praktisert i fylkeskommunen. For å kompensere for denne mulige feilkilden er det i etterkant av de forskjellige temaene i spørreundersøkelsen lagt inn åpne «bokser» hvor respondenten selv har mulighet til å gi tilbakemelding.

For at respondentene skulle ha så lik oppfattelse av begreper og meningen med de forskjellige spørsmålene ble det lagt til forklarende tekst på mange av spørsmålene. Allikevel kan man ikke utelukke at alle respondentene har hatt lik oppfattelse av spørsmålsformuleringen, dette kan ha påvirket svarene som har kommet frem. Det er ikke mulig å garantere at alle informantene har gitt oppriktige og ærlige svar. Men det heller ingen grunn til å tro det motsatte.

Det har det vært viktig å se i flere retninger etter relevante kilder i et forsøk på å få resultatet av oppgaven til å bli mest mulig valid. I tillegg til å foreta valg av respondenter til spørreundersøkelsen er det blitt gjennomført dokumentstudier og litteratursøk. Dette ved gjennomgang av blant annet rapporter, artikler og tidsskrifter. En naturlig gyldighetstest vil være å sjekke egne konklusjoner mot andre undersøkelser. (Jacobsen, 2000) ved å sammenligne svarene fra oppgavens spørreundersøkelse med besvarelser og konklusjoner som kommer fram i Mørketallundersøkelsen™ 2012 kan validitet måles.

Hvilken kunnskap respondenten har om det aktuelle tema, avhenger om respondenten kan mye eller er fersk angående tematikken. Vanligvis er en respondent som kan mye om et tema mer til å stole på enn en som er fersk på området. Validering innebærer også en kritisk drøfting av kildens vilje til i å gi riktig informasjon. Kilder kan ha ulike interesser som kan lede dem til ikke å si hele sannheten. Forskere må alltid vurdere om de kildene som blir benyttet, har noen motiver for å holde tilbake informasjon og der igjen gi et skjevt bilde av virkeligheten. (Jacobsen, 2000) for oppgavens validering er dette forsøkt innfridd ved å anonymisere respondentene og fylkeskommunen vil det ikke være fult så aktuelt å gi uærlig og uriktig informasjon for å skape et skjeft bilde av virkeligheten.

4.4.2 Reliabilitet

For å styrke troverdigheten blir det brukt flere metoder og ulike datakilder. Påliteligheten av dataene vil være samlet via spørreundersøkelse, litteratur, dokumentstudier. I tillegg kommer mine egne erfaringer som er basert på lang praksis innen fagfeltet. Reliabiliteten i kvantitative undersøkelser regnes normalt for å være god. Et moment som styrker reliabiliteten i denne undersøkelsen er det faktum at respondentene har tastet inn svarene direkte inn i Questback. Muligheten for inntastingsfeil som kan skje når noen har punchet inn alle dataene fra papirbesvarelser er dermed eliminert.

De samme spørsmålene ble stilt til alle respondentene, ved de åpne spørsmålene var det ønskelig at respondentene skulle svare så fritt som mulig. Ved mange forskjellige svar kan det være vanskelig å få akkurat de samme svarene dersom undersøkelsene gjentas flere ganger, hvilket i utgangspunktet er nødvendig for å oppnå høy reliabilitet. Ved ren kvantitative undersøkelser er dette i større grad mulig. Jacobsen (2000) mener også åpne spørsmål kun bør benyttes i to tilfeller: ved så mange svaralternativer at man trenger flere sider til å liste dem opp. Eller ved ikke å ha oversikt over alle tenkelige svaralternativer. Spesielt det siste er gjeldende for denne oppgaven.

Det er nødt til å settes lit til at hver enkelt ga oppriktige og ærlige svar på spørsmålene. Når det gjelder pålitelighet og troverdighet av dataene, kan jeg ikke vite hundre prosent sikkert hvem som fylte ut skjemaene. Men jeg antar at det ble fylt ut av dem som fikk e-post med link til spørreskjema. Om undersøkelsene skulle bli gjentatt i nær fremtid, med de samme respondentene, mener jeg at resultatene vil bli tilnærmet det samme. Slik jeg vurderer det er empirien reliabel.

4.5 Metodekritikk

Mine metodevalg ville jeg egentlig gjort noe annerledes, jeg hadde en klar oppfattelse av hvilke spørsmål jeg ville ha besvart før jeg fant relevant teori. Skulle jeg ha gjort oppgaven på ny ville jeg ha gjort en del annerledes. Det viste seg også at det var vanskelig å få de respondentene jeg ønsket. Andre utfordringer var å få respondentene til å utdype tilleggskommentarer i etterkant av hvert tema i spørreundersøkelsen. En spørreundersøkelse gir muligheten til å samle inn forholdsvis mange respondere på relativt kort tid. Dette er en enkel framgangsmåte, men datatilgjengelighet er et problem fordi at det muligens ikke får nok svar for danne et riktig bilde av virkeligheten. Med bakgrunn i datatilgjengelighet har oppgaven dreid fra av hvilket fokus IKT beredskap har i fylkeskommunen generelt, til å gjelde tre fylkeskommuner.

Siden spørreundersøkelsen er anonym både av respondent og fylkeskommune vil den ikke være etterprøvbar. Ideelt sett når formålet med en studie er å studere personers handlinger og holdninger burde det heller blitt benyttet observasjonsdata, i denne forskningen ville dette bli altfor tidkrevende. Det folk faktisk gjør, og det de sier de gjør, kan være to forskjellige ting. Begrunnelsen for å tro det er valide data som har kommet fram er anonymiteten. Det kan være lettere å svare eller kommentere når respondenten vet dette ikke vil falle tilbake på vedkomne.

Avgrensningen til gitt gruppe respondentene mener jeg er god i forhold til problemstillingen, men ved en større studie kunne det være inntresant å benytte respondenter innenfor området «fagansvarlige». (Dette er som oftest enkelt personer som har ansvar for vedlikehold av et fagsystem, for eksempel lønnssystem eller arkivsystem). Disse personene arbeider ikke på IT avdelingen, men på den enkelte avdeling som benytter fagsystemet. Siden fylkeskommunen har et utall av forskjellige fagsystemer ville det vært vanskelig å få kontakt med relevante respondenter på relativt kort tid som dette studiet inkluderer. Det kunne også vært interessant å inkludere respondenter fra andre avdelinger som har arbeidsoppgaver i fagområdet sikkerhet og beredskap.

5 EMPIRI

I dette kapittel blir resultatene fra spørreundersøkelsen presentert. Innledningsvis inneholder kapittelet beskrivelse av og funn fra Mørketallundersøkelsen™ 2012 som er relevante i forhold til oppgaven. Resultatene vil være systematiser etter tema som interne IKT lover og regler, IKT sikkerhetsstyring, risiko og sårbarhetsanalyser (ROS), IKT beredskapsarbeid og IKT øvelse.

5.1 Mørketallsundersøkelsen

Mørketallundersøkelsen™ 2012 vil bli benyttet som «bakteppe», med bakteppe så menes besvarelsene i min spørreundersøkelse vil bli stett i lys av de forskjellige funn i undersøkelsen.

Mørketallsundersøkelsen™ 2012 er beskrevet i kapittel 1.1. Alle besvarelsene er anonymisert slik at verken respondenter eller deres virksomheter har mulighet til å bli identifisert. Spørreundersøkelsen er gjennomført elektronisk av TNS Gallup i april 2012. Tidsrommet for kartleggingen er 2011. Analysen er utført av Datakrimutvalget. *«Datakrimutvalget ble nedsatt ved kongelig resolusjon 11. januar 2002 og skal i første fase av sitt arbeid utrede hvilke endringer som må til i norsk rett for å gjennomføre Europarådskonvensjonen om IKT-kriminalitet – det vil si kriminalitet knyttet til informasjons- og kommunikasjonsteknologi – og foreslå bestemmelser som tilfredsstiller konvensjonens krav. Dette innebærer at det blant annet må gis regler om pålegg om sikring av data, samt eventuelt fastsettes en generell plikt til å lagre trafikkdata for et bestemt tidsrom. I andre fase av arbeidet står Datakrimutvalget nokså fritt til å vurdere andre lovgivningsspørsmål, både etter straffeloven og straffeprosessloven.» (*NOU 2003: 18)

Mørketallundersøkelsen™ 2012 har en sentral plass i opplysnings og informasjonsstrategien mot næringslivet og offentlige myndigheter. Undersøkelsen viser at det er et større gap enn tidligere mellom trusler og sikkerhetstiltak blant norske virksomheter parallelt med at IT-avhengigheten øker. Norske virksomheter, særlig ledere, mangler kunnskap om informasjonssikkerhet og har ikke oversikt over trusler og hendelser. Blant daglige ledere er det 66 % som bekrefter at de gjennomfører risikoanalyser, og hele 20 % som ikke vet om det gjennomføres risikoanalyser. *«Dette er svært bekymringsfullt med tanke på at daglig leder har overordnet ansvar for sikkerheten i virksomheten»* (Mørketallundersøkelsen™ 2012 s25)
Dette kan forklare at mange virksomheter ikke har tatt i bruk tilgjengelige sikkerhetstiltak og heller ikke fokusert på sikkerhetskultur. Aktuelle hovedfunn er som følger:

- *Bare 1 av 6 virksomheter har retningslinjer for gjennomføring av verdivurdering.*
- *Av daglig ledere, som er øverste ansvarlige for sikkerhet og beredskap, svarer 1 av 5 at de ikke vet om det gjennomføres risikoanalyser i egen virksomhet.*
- *12 % av de som har opplevd en hendelse har ikke fulgt opp med forbedringstiltak*

for å forebygge nye hendelser.

- *Bare 1 av 3 virksomheter har beredskapsplaner. Av disse igjen er det 1 av 3 som har krav til at det gjennomføres øvelser.*
- *1 av 3 virksomheter vet ikke kostnaden knyttet til sikkerhetshendelser.*

Ovenfor liggende funn er av alle besvarelsene som ble mottatt etter undersøkelsen. For å finne besvarelser som kunne sammenlignes med mine funn, var det en nødvendighet å kunne filtrere vekk alle besvarelser som ikke omhandlet fylkeskommunen.
Ved henvendelse til ansvarlig for Mørketallundersøkelsen™ 2012 med spørsmål om det var mulighet med den type filtrering av datagrunnlaget, ble jeg videreformidlet til kontaktet ved TNS gallup. Deretter fikk jeg tilsendt fil med filtrert besvarelse bare fra offentlig sektor. For å komme nærmest mulig en sammenligning av mine respondenter er det ut fra denne filen blitt filtrert vekk alle virksomheter unntagen:

- Generell offentlig administrasjon
- Videregående opplæring innen allmennfaglige studieretninger
- Videregående opplæring innen tekniske og andre yrkesfaglige

Videre er det filtrert ut alle yrkesgrupper unntagen:

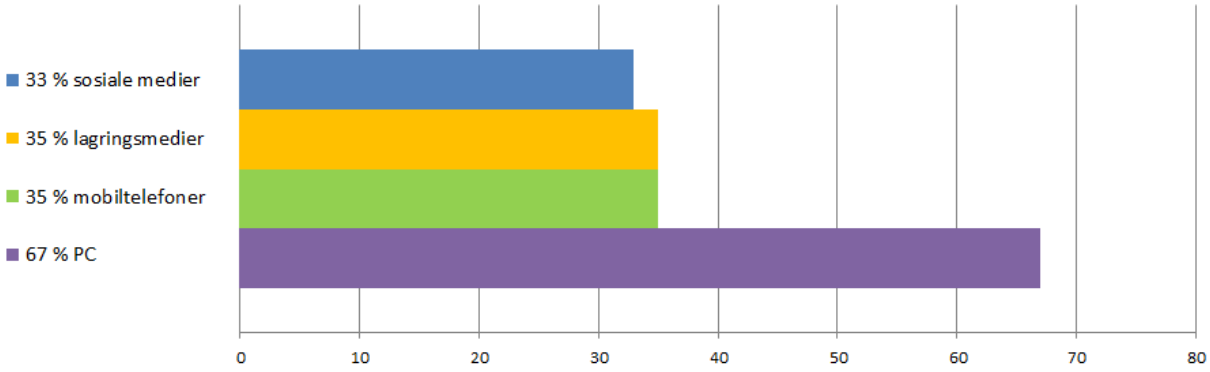
- IT-ansvarlig
- Sikkerhetsansvarlig
- Daglig leder

Disse filtreringene anser jeg som så lik som mulig fylkeskommunal organisasjon. Offentlig administrasjon kan også være annet enn fylkeskommunens administrasjon, dette ble tatt med på bakgrunn av antatte like utfordringer. Videregående opplæring er det bare fylkeskommunen som besettinger. Yrkesgruppene anser jeg som relevante når det gjelder mine respondenter. Funn fra disse filtreringene vil være informative og bli benyttet som et bakteppe til mine funn. Videre i kapittelet følger filtrerte funn fra undersøkelsen.

5.1.1 Interne IKT lover og regler

«Virksomheter i Norge tar i bruk mer teknologi, spesielt e-post på mobiltelefoner, og er mer aktive på sosiale medier, men mangler ofte retningslinjer.»
(Mørketallundersøkelsen™ 2012 s. 8)

96 % svarer de benytter virksomheten trådløs nettverkstilgang (Wi-Fi)
88 % svarer de mottar virksomhetens e-post på mobilen.
På spørsmål om virksomheten har sikker bruk i form av skriftlige utarbeidet retningslinjer og prosedyrer for behandling av informasjon svarer følgende 33 % sosiale medier, 35 % mobiltelefoner, 35 % lagringsmedier og 67 % PC som vist under i figur 5.1



Figur 5.1 Retningslinjer og prosedyrer for behandling av informasjon

«Vi er også urolige for utviklingen med mangel på retningslinjer i offentlig sektor. Dette kan medføre en dårligere evne til å detektere og spore sikkerhetsbrudd, og derved større sårbarhet for hendelser.» (Mørketallundersøkelsen™ 2012 s. 23)

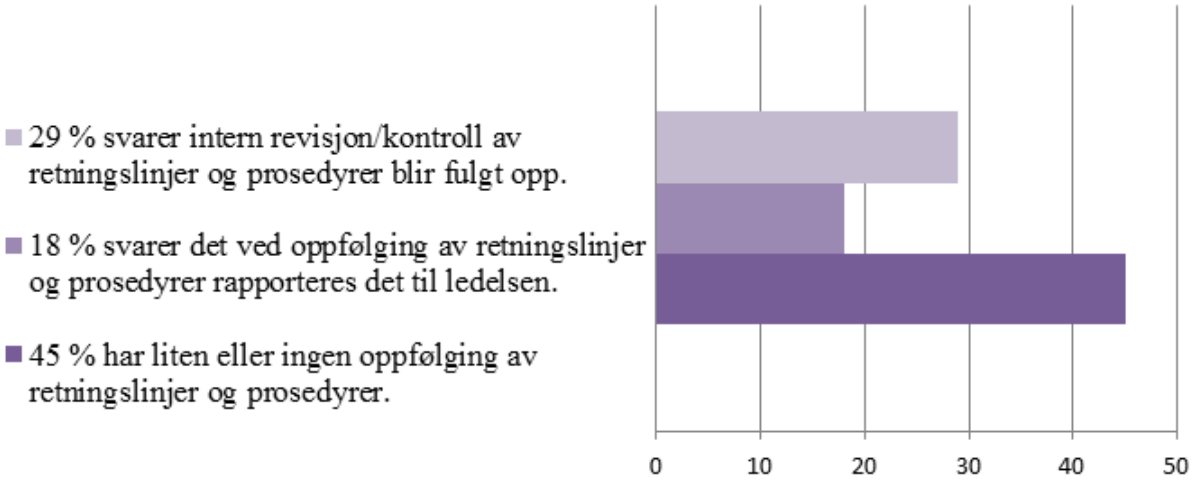
Bruk av privateid utstyr til virksomhetsinformasjon er økende. Dette medfører en ny risiko for norske virksomheter. Privateid utstyr brukes i mange flere sammenhenger, og er koblet til flere ulike nettverk. Dette gjør det vanskeligere å beskytte mot angrep. Bruk av privateid utstyr vanskeliggjør også rapportering og kontroll over informasjonen.
37 % svarer det foreligger retningslinjer for bruk av privateid utstyr, og bedriften tillater behandling eller lagring av virksomhetsinformasjon på privateid utstyr.

53 % svarer at de ikke tillater kunder, samarbeidspartnere eller leverandører tilgang utenfra (via internett) til virksomhetens IT-systemer.

5.1.2 IKT sikkerhetsstyring

Trusselbildet forandrer seg raskt. Angrepene rettes i større grad mot mennesker og ikke teknologi. Det er viktig å etablere en god sikkerhetskultur i virksomheten.
Undersøkelsen viser at halvparten av de rapporterte sikkerhetshendelsene kan spores tilbake til egne ansatte eller innleid personell. Dette kan skyldes både tilfeldige feil grunnet manglende opplæring og mer målrettede handlinger.
22 % oppgir opplæring i sikker bruk av IT regelmessig gjennom ansettelsesperioden.
41 % svarer de må undertegne retningslinjer for bruk av IT-systemer.

Som det fremkommer av figur 5.2 svarer 29 % at intern revisjon eller kontroll av retningslinjer og prosedyrer blir fulgt opp. Videre svarer 18 % ved oppfølging rapporteres det til ledelsen. Derimot er det 45 % som har liten eller ingen oppfølging av retningslinjer og prosedyrer. Som vist i Figur 5.2 Intern revisjon/kontroll av retningslinjer under.



Figur 5.2 Intern revisjon/kontroll av retningslinjer.

Videre oppgir 82 % at rapportering eller varsling fra egne ansatte som viktigste kilder til å oppdage sikkerhetshendelser.

5.1.3 Risiko og sårbarhetsanalyser (ROS)

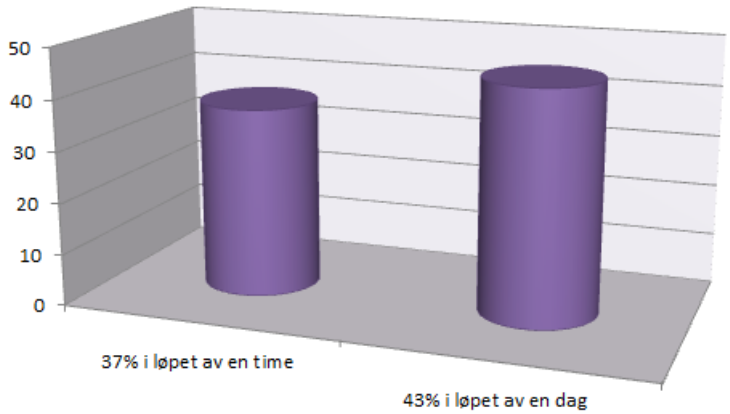
84 % av virksomhetene gjennomfører risikovurderinger av viktige IT-systemer ved anskaffelse eller betydelige endringer. Det er kun 20 % av disse som gjennomfører risikoanalyser hver gang det innføres nye løsninger.

På spørsmål om hvor ofte gjøres det risikovurderinger oppgir 29 % at risikovurderinger blir gjort jevnlig i hend hold til etablerte rutiner. 45 % oppgir at det gjøres risikovurderinger av og til, avhengig av hvilke løsninger det er snakk om.

5.1.4 IKT Beredskapsarbeid

«De som foretar risikovurderinger av viktige IT-systemer er mer forberedt og sterkere på beredskap. Av de som har foretatt en risikovurdering har 44 % laget planer for håndtering av de viktigste informasjonssikkerhetshendelsene, i motsetning til 15 % hos de som ikke har foretatt en risikovurdering.» (Mørketallundersøkelsen™ 2012 s. 20)

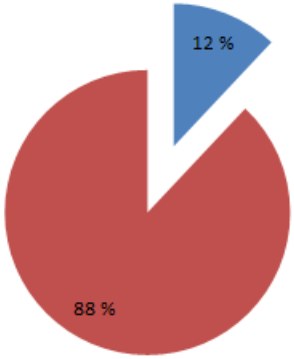
På spørsmål om hvor lang tid vil det ta før det skaper alvorlige konsekvenser for virksomheten dersom de viktigste IT-systemene er ute av drift. Svarer 37 % i løpet av 1 time og 43 % i løpet av 1 dag, dette er vist i figur 5.3 under.



Figur 5.3 Alvorlige konsekvenser dersom viktigste IT-systemene er ute av drift.

5.1.5 IKT øvelse

Som vist i figur 5.4 under har 12 % krav til gjennomføring av systematiske øvelser knyttet til IT-beredskap.



Figur 5.4 Krav til gjennomføring av systematiske øvelser knyttet til IT-beredskap.

Noen andre funn som ikke er direkte knyttet til momenter av mine forskningsspørsmål men som jeg mener er vesentlig betydning for det totale bilde:

På spørsmål om hvordan er IT-driften organisert i virksomheten svarer 37 % som del av egen virksomhet med egne ansatte. På spørsmål om tyveri av IT-utstyr (PC, server, Nettbrett, Smarttelefoner etc.) av 49 spurte virksomheter svarer de samlet 51 hendelser (dette er totalt antall anmeldte hendelser) i 2011.
På spørsmål om estimert total nedetid på sentrale IT-systemer i 2011 som følge av informasjonssikkerhetshendelser svarer 14 % Inntil 1 dag, 12 % Inntil 1 time og 33 % vet ikke.
«Av de som oppgir å få problemer innen én time om IT-systemet var nede, er det svært bekymringsfullt at bare 43 % har etablert beredskapsplaner for håndtering av de viktigste informasjonssikkerhetshendelsene. Den samme gruppen er enda svakere på systematiske øvelser knyttet til IT-beredskap. Bare 15 % har krav om øvelser.»
(Mørketallundersøkelsen™ 2012 s. 20)

5.2 Spørreundersøkelsen

I tillegg til de 27 spørsmålene var det ønskelig med tilbakemeldinger i form av kommentarer med den hensikt å få fram momenter som ikke kom fram i de stilte spørsmålene. Totalt var det 6 åpne spørsmål hvor respondenten selv måtte taste inn svaret. I tillegg var det 5 spørsmål som omhandlet respondentens personalia. Det vil si totalt 38 spørsmål i min spørreundersøkelse.
De åpne spørsmålene var alle plassert på slutten av hvert spørsmålstema. Og et til slutt i undersøkelsen etter siste spørsmål med svaralternativer var det var ønskelig med tilbakemelding fra respondentene om de hadde andre kommentarer når det gjelder IKT sikkerhet og beredskapsarbeid i fylkeskommunen. Dette er tidligere beskrevet mer utfyllende i kapittel 4.3.3 Spørreundersøkelsen.

5.2.1 Respondentene

Som nevnt tidligere er mine alle respondenter ansatt i fylkeskommunen og har hver sine arbeidsoppgaver, prioriteringer og ansvar. Felles for alle stillingsgruppene vil være at de vil bli berørt i forhold til oppgavens problemstilling. På bakgrunn av dette var det helt naturlig å gi alle respondentene like spørsmål.

Rådmann
Beskrivelse av fylkeskommunens historie, funksjoner og organisasjon og politiske relasjoner samt rådmannens oppgaver er godt beskrevet utfyllende i kapittel 2 Fylkeskommunen. I kapittel 4.2.1 er det beskrevet hvilke utfordringer rådmann står ovenfor.
På forespørsel om å være respondent i min masteroppgave var det to rådmenn som svarte positivt på min forespørsel. Den ene hadde ansettelse mindre enn 2år og den andre mellom 2 og 8 år i nåværende stilling og fylkeskommunen totalt. Angående spørsmål som omhandlet relevant utdannelse med vitnemål eller kurs knyttet til IKT sikkerhet og beredskap, hadde ingen av rådmennene utdannelse med vitnemål, eller relevante kurs.

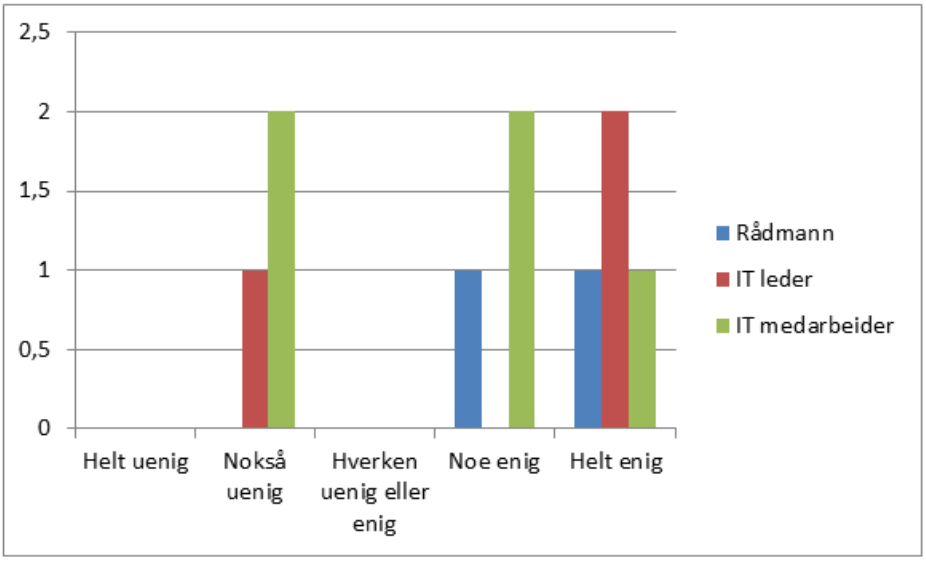
IT Leder
IT leder er den øverste lederen for IT avdelingen/enheten i fylkeskommunen. Hvilke forventninger og oppgaver som tilfaller IT leder er godt beskrevet i kapittel 4.2.1. Spesielt med tanke på spesielle utfordringer ved å være «mellom barken og veden». ("Jf." Kap.3.1.1)
På forespørsel om å være respondent i min masteroppgave var det tre IT ledere som svarte positivt på min forespørsel. Alle hadde ansettelse mer enn 8 år i nåværende stilling. Angående spørsmål som omhandlet relevant utdannelse med vitnemål eller kurs knyttet til IKT sikkerhet og beredskap, hadde en av IT lederne utdannelse med vitnemål i informatikk, på spørsmål om relevante kurs var det en som hadde dagskurs/seminar.

IT Medarbeider
IT medarbeider er ansatt som arbeider på IT avdelingen eller enheten i fylkeskommunen. Hvilke forventninger og oppgaver som tilfaller IT medarbeider er godt beskrevet i kapittel 4.2.1. Spesielt med tanke arbeidsoppgaver angående drift og vedlikehold av IT systemer.
På forespørsel om å være respondent i min masteroppgave var det fem IT medarbeidere

som svarte positivt på min forespørsel. På spørsmål angående ansettelse tid i fylkeskommunen, var det to respondenter med mindre enn 2 år, to mellom 2 til 8 i nåværende stilling. Det var en som hadde ansettelse mer enn 8 år i fylkeskommunen. Spørsmål som omhandlet relevant utdannelse med vitnemål eller kurs knyttet til IKT sikkerhet og beredskap, var det tre IT medarbeidere som hadde utdannelse i informatikk og to som hadde relevante kurs.

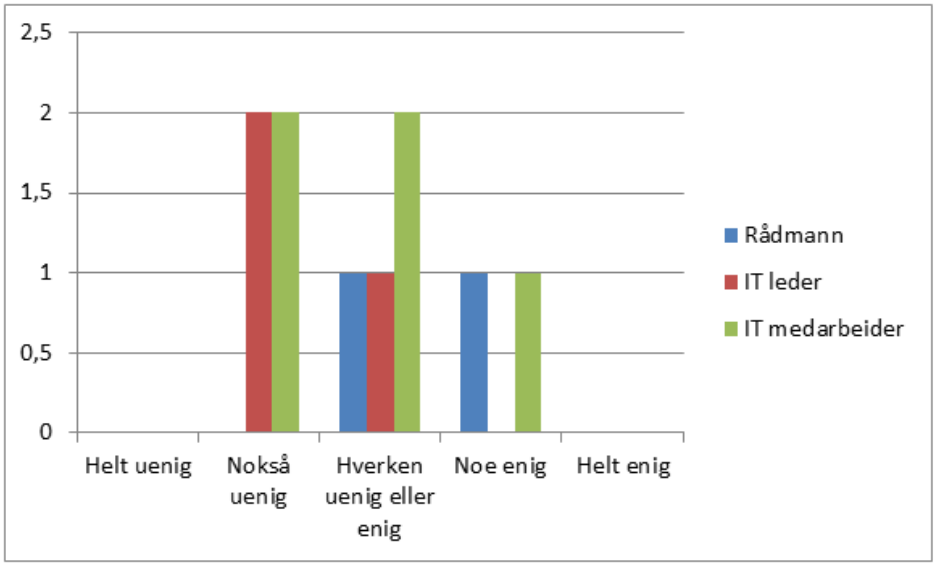
5.2.2 Fylkeskommunens interne IKT lover og regler

På spørsmål om det foreligger et fullverdig IKT lovverk fra internt hold. Med «fullverdig IKT lovverk» menes lovverk som ivaretar håndtering av for eksempel epost, passord, bruk av bærbar PC og telefon. Totalbesvarelsen varierer noe, 3/10 (en IT leder og to IT medarbeidere) svarer «nokså uenig». Hovedtyngden av respondentene 7/10 (begge rådmenn, to IT ledere og tre IT medarbeidere) svarer de er enige (i mer eller mindre grad). Resultatene er vist i figur 5.5 under.



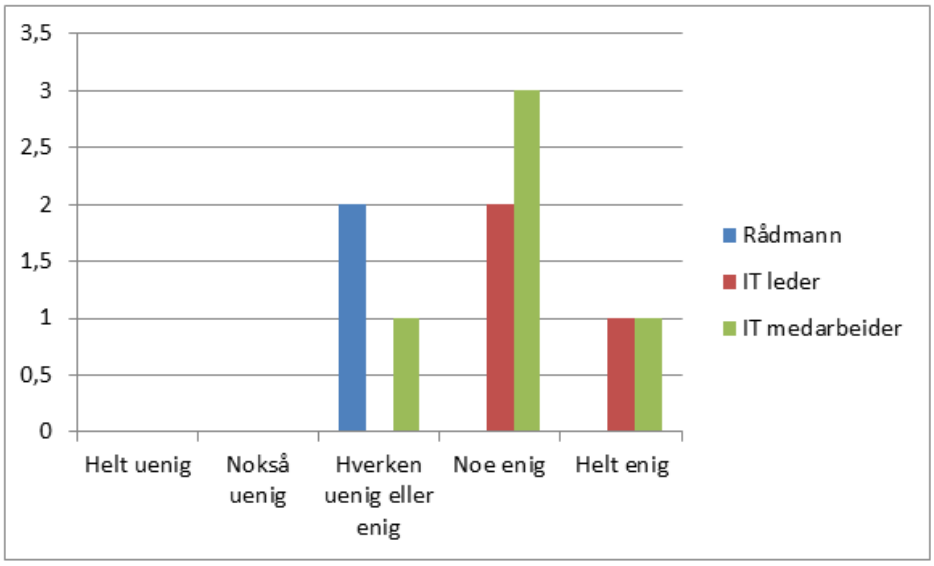
Figur 5.5 Det foreligger et fullverdig IKT lovverk fra internt hold

På spørsmål om IKT lovverket blir ikke overholdt, varierer totalbesvarelsen noe. 4/10 (to IT ledere og to IT medarbeidere) svare «nokså uenig». 4/10 (en rådmann, en IT leder og to IT medarbeidere) svarer «hverken uenig eller enig» resterende 2/10 (en rådmann og en IT medarbeider) svarer de er enig (i mer eller mindre grad). Resultatene er vist i figur 5.6 under.



Figur 5.6 IKT lovverket blir ikke overholdt.

På spørsmål om kvalitetssikring av eget arbeid med IKT sikkerhet og beredskap blir fulgt opp av interne tilsyn, med «interne tilsyn» menes for eksempel egen arbeidsgruppe på tvers av fagområder eller personer som ikke direkte er med på utformingen av IKT sikkerhet og beredskaps arbeidet. Som det går fram av figur 5.7 under svarer 3/10 (begge rådmenn og en IT medarbeider) svarer «hverken uenig eller enig». Oppfattelsen er annerledes hos IT ledere og IT medarbeidere. 7/10 (alle IT lederne og fire IT medarbeidere) svarer «enig» (i mer eller mindre grad). Resultatene er vist i figur 5.7 under.



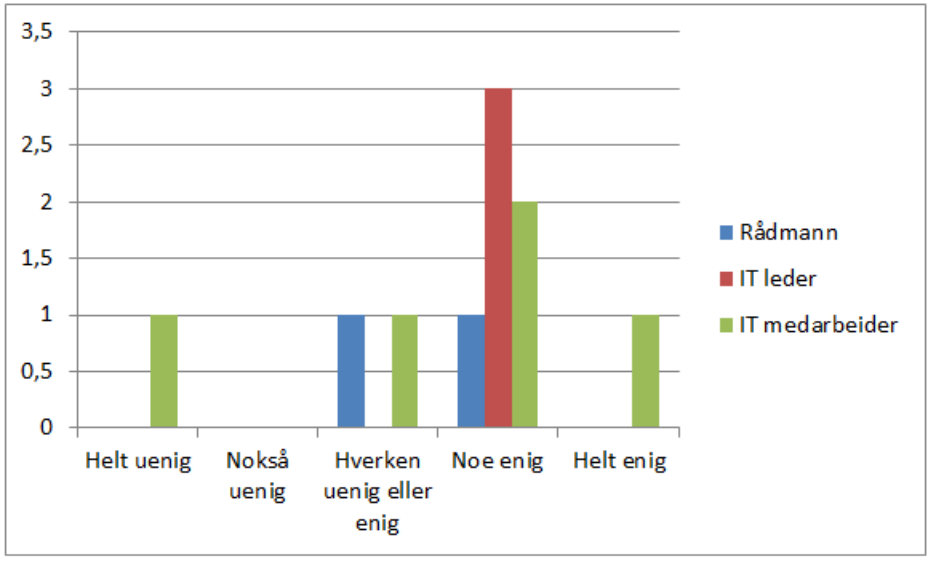
Figur 5.7 Kvalitetssikring av eget arbeid blir overholdt og fulgt opp av interne tilsyn.

På det nevnte åpne spørsmålet, som var etter hvert av spørsmålstemaene der respondenten ble bedt om å utdype eller komme med kommentarer i dette tilfelle fylkeskommunens interne IKT lover og regler. Var det ingen av rådmennene som hadde

noen kommentar. To IT ledere hadde følgende kommentarer *« Fylkeskommunen har et styrings- og kvalitetsprosjekt hvor arbeidsprosesser/tjenester skal risikovurderes opp mot lover og regler.»* og *«Har etablert formelt ansvar og organisering innen personvern og IKT-sikkerhet. Har hatt tilsyn fra Datatilsynet 2 ganger de siste 4 år, mindre avvik er fulgt opp og nå i orden.»* To IT medarbeidere hadde følgende kommentarer *«alt kan gjøres bedre, men vi har internt regelverk som blir revidert og fulgt opp ved tilsyn og kontroller.»* Og *«går ut fra at "IKT lover og regler" er det samme som vi kaller "policy" internt hos oss (passordpolicy, ikke sende sensitive personopplysninger i epost, ROS analyse ved innføring av nye system, osv.)* »

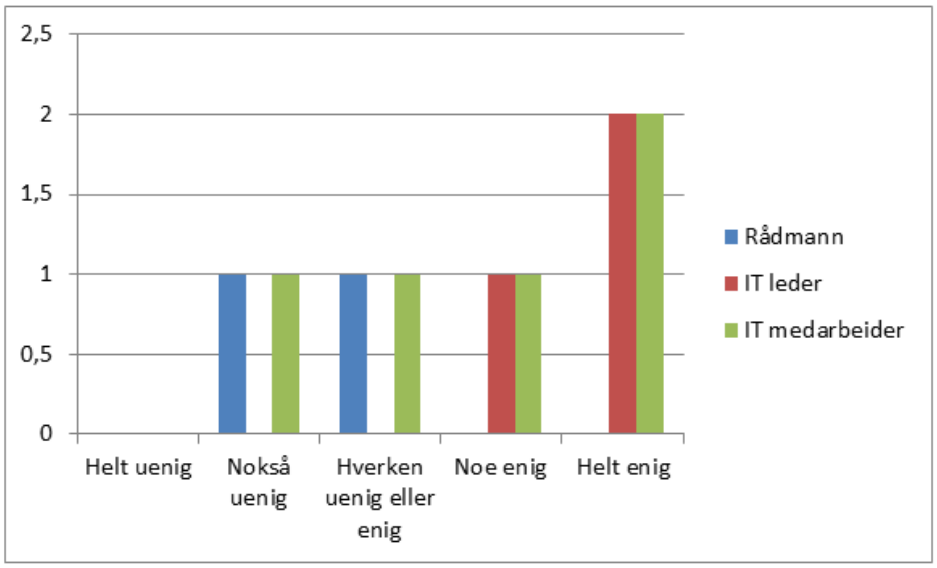
5.2.3 IKT sikkerhetsstyring

På spørsmål om IKT beredskap er synliggjort og kommunisert til ansatte fra ledelsen. Med «Synliggjort og kommunisert til ansatte» menes at ansatte mottar og forstår budskapet. Her varierer totalbesvarelsen noe. 1/10 (IT medarbeider) som svarer «helt uenig», 2/10 (en rådmann og en IT leder) svarer «hverken uenig eller enig».
Selv om totalbesvarelsen varierer noe ser det ut som hovedtyngden av respondentene 7/10 (en rådmann, alle IT lederne og tre IT medarbeidere) svarer de er enige (i mer eller mindre grad). Resultatene er vist i figur 5.8 under.



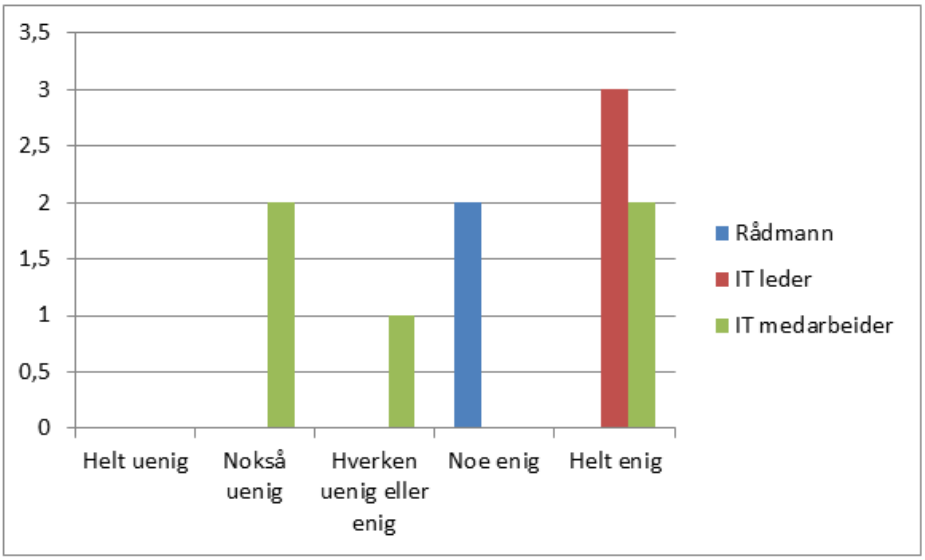
Figur 5.8 IKT-beredskap er synliggjort og kommunisert til ansatte fra ledelsen.

På spørsmål om IKT sikkerhet og beredskap er synliggjort og kommunisert hos ledelsen. «Synliggjort og kommunisert hos ledelsen» menes at ledelsen får tilbakemelding fra medarbeidere. Her varierer totalbesvarelsen noe, 2/10 (rådmann og IT medarbeider) svarer «nokså uenig». 2/10 (rådmann og IT medarbeider) svarer «hverken uenig eller enig». Selv om totalbesvarelsen varierer noe ser det ut som hovedtyngden av respondentene 6/10 (alle IT lederne og tre IT medarbeidere) svarer de er enige (i mer eller mindre grad). Resultatene er vist i figur 5.9 under.



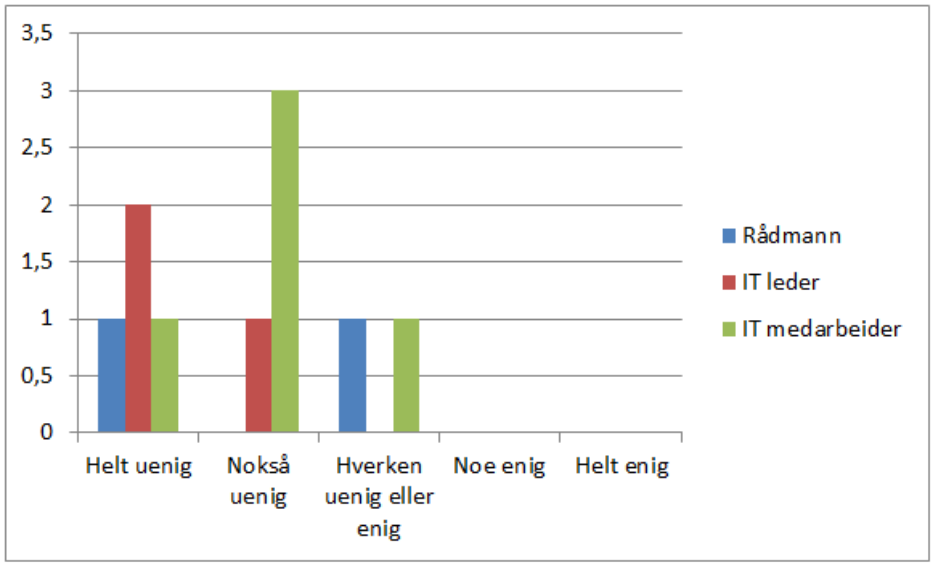
Figur 5.9 IKT sikkerhet og beredskap er synliggjort og kommunisert hos ledelsen.

På spørsmål om IKT beredskapsarbeid vektlegges i internkontrollsystemet, varierer totalbesvarelsen noe, 2/10 (IT medarbeidere) er «nokså uenig». 1/10 (IT medarbeider) er «hverken uenig eller enig». Derimot besvarelsen fra 7/10 (begge rådmenn, alle IT lederne og to IT medarbeidere) er enig (i mer eller mindre grad). Resultatene er vist i figur 5.10 under.



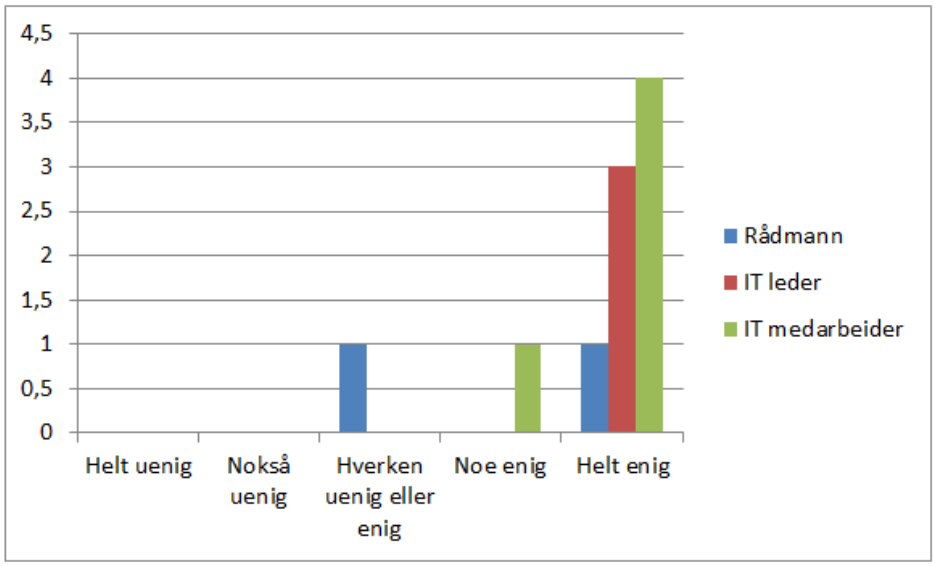
Figur 5.10 IKT beredskapsarbeid vektlegges i internkontrollsystemet.

På spørsmål om sikkerhet og IKT beredskap er ikke tema på møter, samlinger e.l. Hovedtyngden av respondentene 8/10 svarer uenig (i mer eller mindre grad). Resterende 2/10 (rådmann og IT medarbeider) er «hverken uenig eller enig». Resultatene er vist i figur 5.11 under.



Figur 5.11 Sikkerhet og IKT beredskap er ikke tema på møter, samlinger e.l.

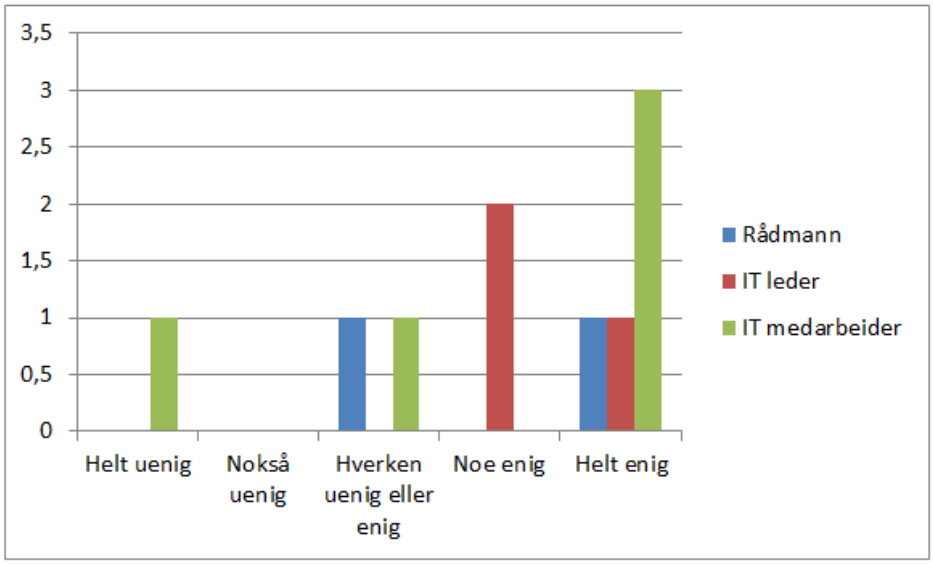
På spørsmål om delaktighet i arbeidsoppgaver som omfatter IKT beredskapsarbeidet, varierer totalbesvarelsen ikke så mye. 1/10 (rådmann) svarer «hverken uenig eller enig». Resterende 9/10 (en rådmann, alle IT lederne og alle IT medarbeiderne) har samme oppfattelse det vil si hovedtyngden av respondentene, svarer at de er delaktighet i arbeidsoppgaver som omfatter IKT beredskapsarbeidet. Det vil si alle unntagen en rådmann er delaktig i disse arbeidsoppgavene. Resultatene er vist i figur 5.12 under.



Figur 5.12 Delaktig i arbeidsoppgaver som omfatter IKT beredskapsarbeidet.

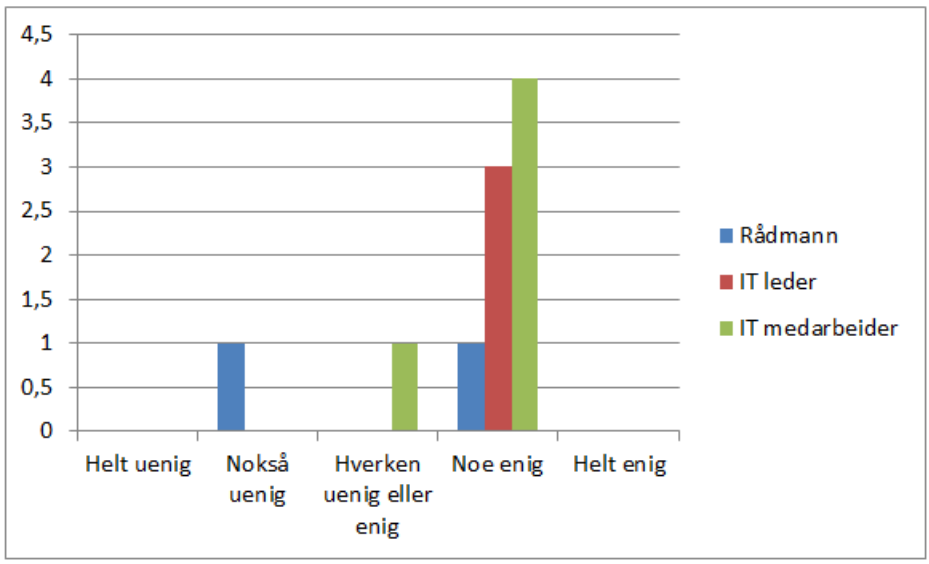
Et annet spørsmål var, «Alle» oppfordres til å komme med sine meninger ang. IKT sikkerhetsarbeidet. Med «alle» menes medarbeidere som arbeider med IKT systemer. Varierer totalbesvarelsen noe, 1/10 (IT medarbeider) svarer «helt uenig». 2/10 (rådmann og IT medarbeider) svarer «hverken uenig eller enig». Selv om totalbesvarelsen varierer noe ser det ut som hovedtyngden av respondentene 7/10 (en rådmann, alle IT lederne og

tre IT medarbeidere) svarer de er enige (i mer eller mindre grad). Resultatene er vist i figur 5.13 under.



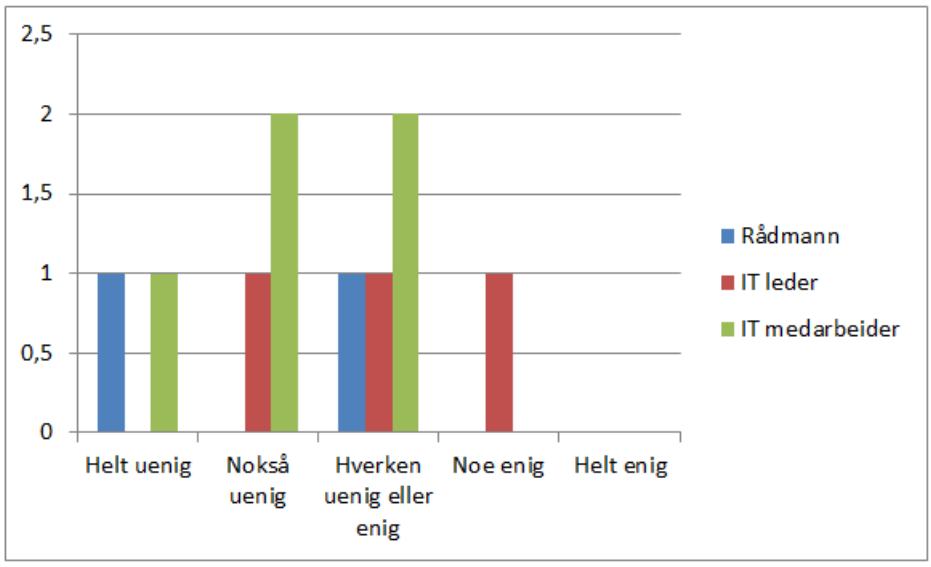
Figur 5.13 «Alle» oppfordres til å komme med sine meninger ang. IKT sikkerhetsarbeidet.

På spørsmål om IKT sikkerhet og beredskap er et ”daglig” tema hos dere, varierer totalbesvarelsen ikke nevneverdig. 1/10 (rådmann) svarer «nokså uenig». 1/10 (IT medarbeider) svarer «hverken uenig eller enig». Hovedtyngden av respondentene 8/10 (en rådmann, alle IT lederne og fire IT medarbeidere) svarer enig (i mer eller mindre grad). Det vil si de fleste mener IKT sikkerhet og beredskap er et ”daglig” tema. Resultatene er vist i figur 5.14 under.



Figur 5.14 IKT sikkerhet og beredskap er et ”daglig” tema hos dere.

På spørsmål om sikkerhet og IKT beredskap formidles ikke eksternt, varierer totalbesvarelsen ganske en del, 5/10 (en rådmann, en IT leder og tre IT medarbeidere) svarer uenig (mer eller mindre grad). 4/10 (en rådmann, en IT leder og to IT medarbeidere) svarer «hverken uenig eller enig» og resterende 1/10 (IT leder) svarer «noe enig»
Resultatene er vist i figur 5.15 under.

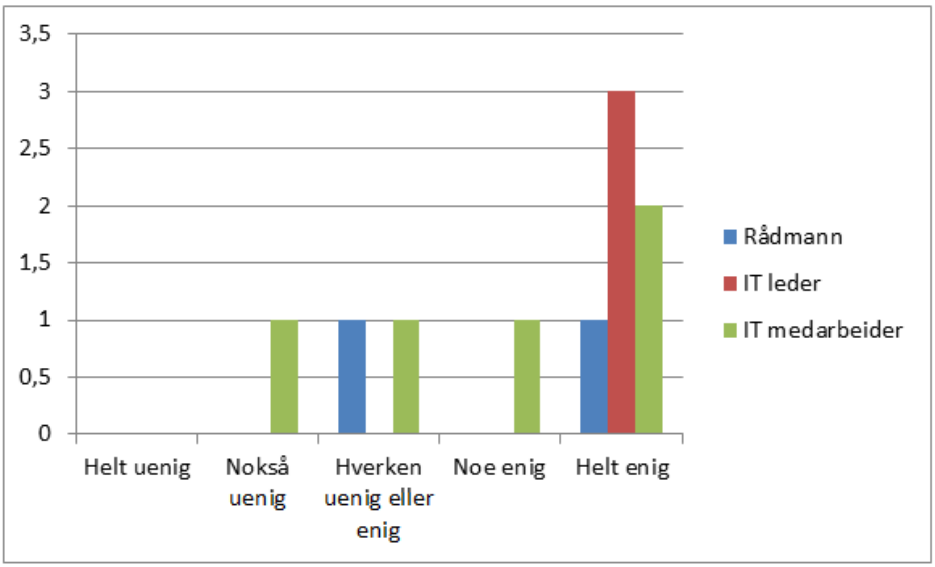


Figur 5.15 Sikkerhet og IKT beredskap formidles ikke eksternt (til lokasjoner som skole og tannhelse).

På det nevnte åpne spørsmålet, som var etter hvert av spørsmålstemaene der respondenten ble bedt om å utdype eller komme med kommentarer i dette tilfelle fylkeskommunens sikkerhetsstyring. Var det ingen av rådmennene som hadde noen kommentar. To IT ledere hadde følgende kommentarer *« har håndbok for info.sikkerhet og personvern, nedsatt sikkerhetsgruppe og har rutiner for årlig sikkerhetsrevisjon.»* og *«det er fortsatt ugjorte oppgaver for å sikre beredskap og sikkerhetsstyring. Dette er et kontinuerlig arbeid som må følges opp over tid.»* Ingen av IT medarbeidere hadde noen kommentarer.

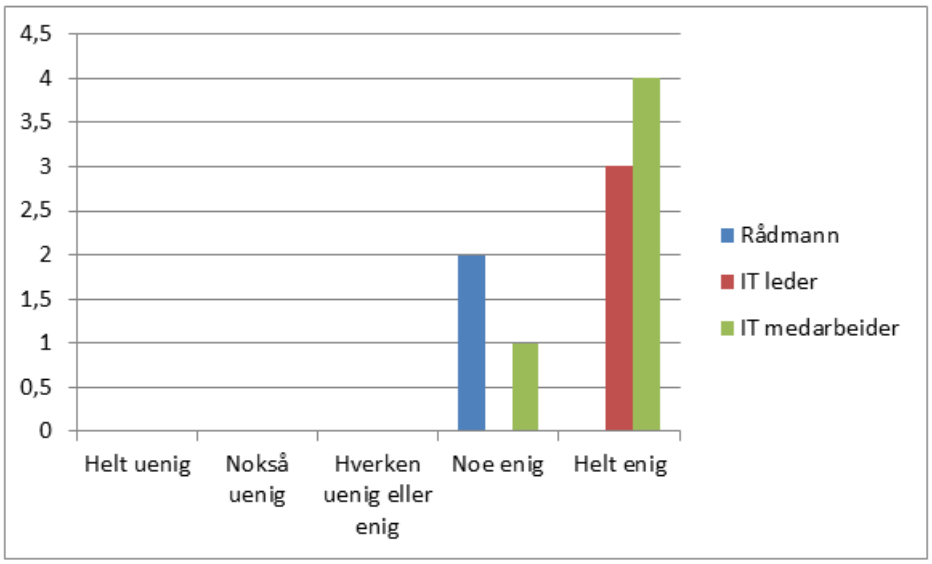
5.2.4 Risiko og sårbarhetsanalyser (ROS)

På spørsmål om utforming av ROS er et samarbeid mellom ansvarlige for IKT systemene og ledelsen. Her varierer totalbesvarelsen noe, 1/10 (IT medarbeider) svarer «nokså enig». 2/10 (En rådmann og en IT medarbeider) svarer «hverken uenig eller enig». Selv om besvarelsen varierer noe ser det ut som hovedtyngden av respondentene 7/10 (en rådmann, alle IT lederne og tre IT medarbeidere) svarer enig (i mer eller mindre grad). Resultatene er vist i figur 5.16 under.



Figur 5.16 Utforming av ROS er et samarbeid mellom ansvarlige for IKT systemene og ledelsen.

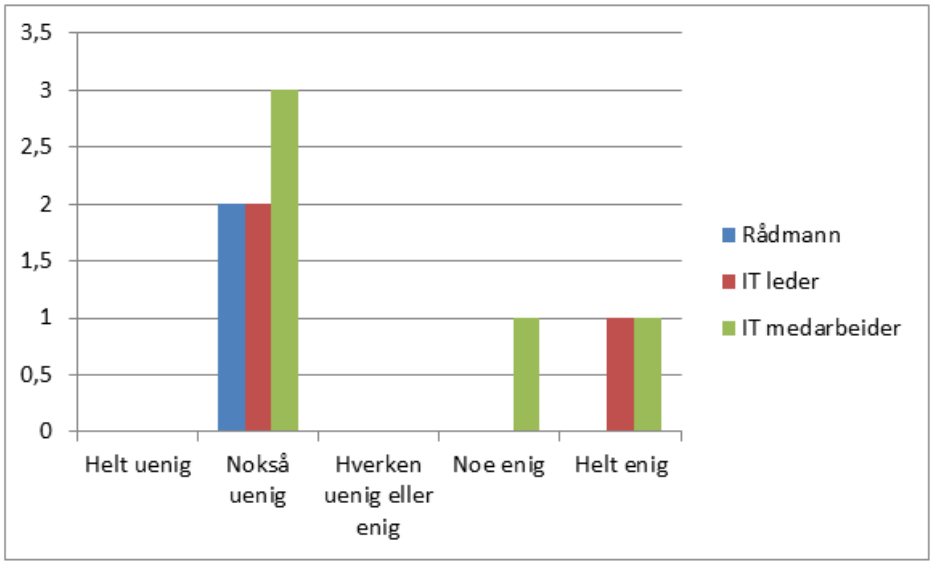
På spørsmål om det er gjort ROS med forskjellige senario. Med «forskjellige senario» menes for eksempel brann i serverrom, strømbrudd over lengere tid, hærverk eller tyveri i serverrom. Her varierer totalbesvarelsen ikke nevneverdig. 10/10 svarer enig (i mer eller mindre grad), det vil si det er gjort risiko og sårbarhetsanalyse med forskjellige senarioer. Resultatene er vist i figur 5.17 under.



Figur 5.17 Det er gjort ROS med forskjellige senario.

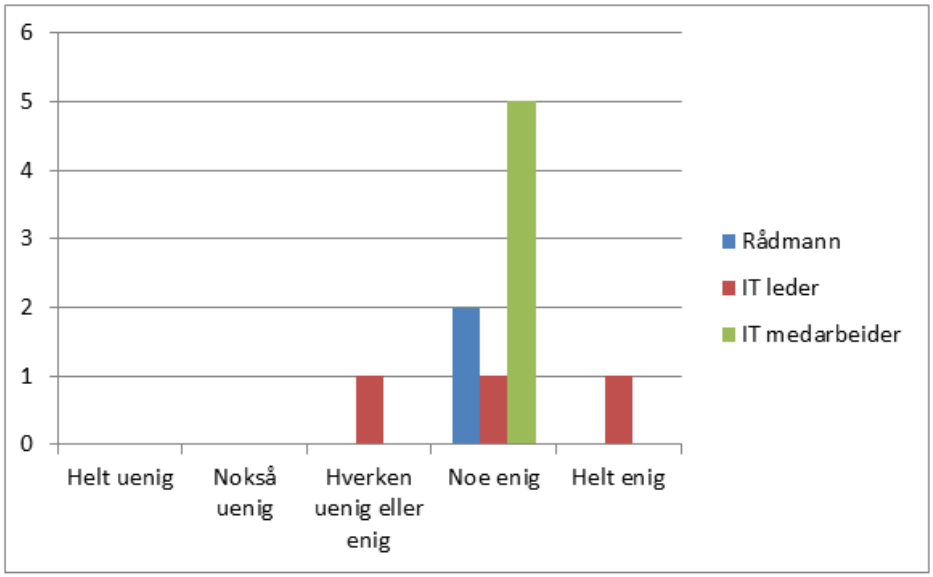
På spørsmål om det er ikke gjort en ansvars fordeling når det gjelder de ulike scenarioene i ROS`en. Med «ansvars fordeling» menes ansvar plassert hos enkelte personer hvis noen av scenarioene skulle inntreffe. Her varierer totalbesvarelsen ikke nevneverdig. Hovedtyngden av respondentene 7/10 (begge rådmenn, to IT lederne og tre IT medarbeidere) svarer «nokså uenige». Resterende 3/10 (en IT leder og to IT

medarbeidere) svarer enig (i mer eller mindre grad). Det vil si de fleste mener det er gjort en ansvars fordeling. Resultatene er vist i figur 5.18 under.



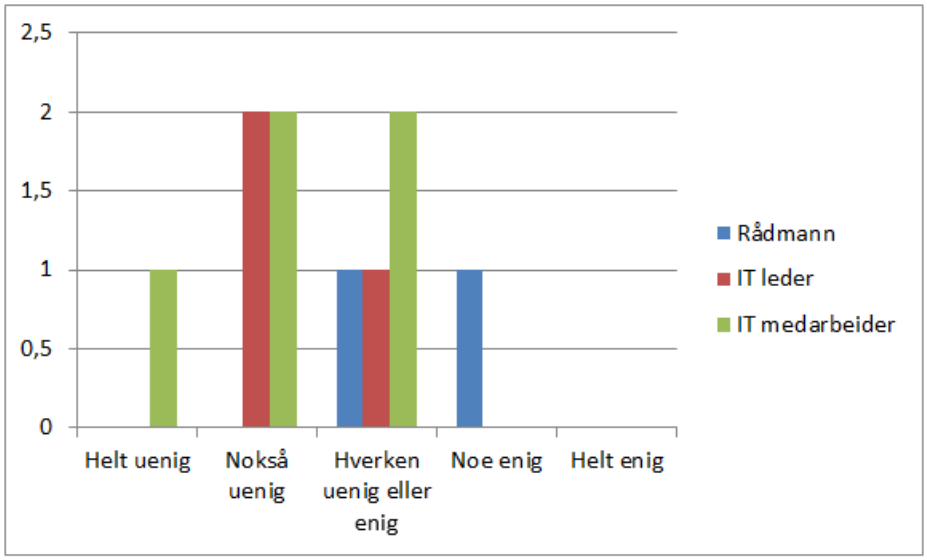
Figur 5.18 Det er ikke gjort en ansvars fordeling når det gjelder de ulike scenarioene i ROS`en.

På spørsmål om det er laget en handlingsplan for å være best mulig rustet i forhold til senarioene, Med «handlingsplan» menes en plan for best mulig å unngå at noen av senarioene inntreffer. 9/10 svarer enig (i mer eller mindre grad), 1/10 (IT leder) svarer «hverken uenig eller enig». Det vil si de fleste svarer det er laget en handlingsplan. Resultatene er vist i figur 5.19 under.



Figur 5.19 Det er laget en handlingsplan for å være best mulig rustet i forhold til senarioene.

På spørsmål om ROS blir ikke gjennomført regelmessig, varierer totalbesvarelsen noe. 5/10 (to IT ledere og tre IT medarbeidere) svarer uenig (i mer eller mindre grad). 4 /10 (en rådmann, en IT leder og to IT medarbeidere) er «hverken uenig eller enig» og resterende 1/10 (rådmann) svarer «noe enig». Resultatene er vist i figur 5.20 under.

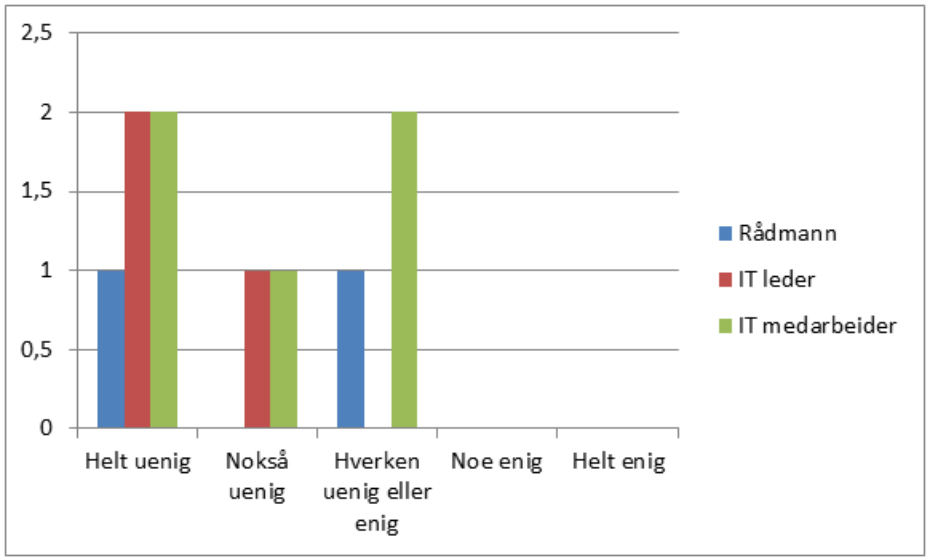


Figur 5.20 ROS blir ikke gjennomført regelmessig.

På det nevnte åpne spørsmålet, som var etter hvert av spørsmålstemaene der respondenten ble bedt om å utdype eller komme med kommentarer i dette tilfelle fylkeskommunens ROS. Var det ingen av rådmennene som hadde noen kommentar. Alle tre IT ledere hadde kommentarer *« ROS er viktig i alle ledd i fylkeskommunale tjenester for å sikre at fylkeskommunen gir gode nok tjenester samt være proaktiv ovenfor uheldige hendelser. Tiltak grunnet ROS er viktig å få fremmet i økonomiplanarbeidet.», «vi har gode maler og bra basisvurderinger »* og *«en ting er å analysere, noe annet er å få etablert tiltak for å redusere/minimere risiko. Det gjenstår å etablere fullverdig backup site for å kunne håndtere en krise.»* En IT medarbeider hadde følgende kommentar *«Det blir gjennomført ROS-analyser ved nye løsninger og konfigurasjonsendringer. Jevnlig (om ikke særlig hyppig) for systemer/løsninger hvor det behandles sensitiv informasjon.»*

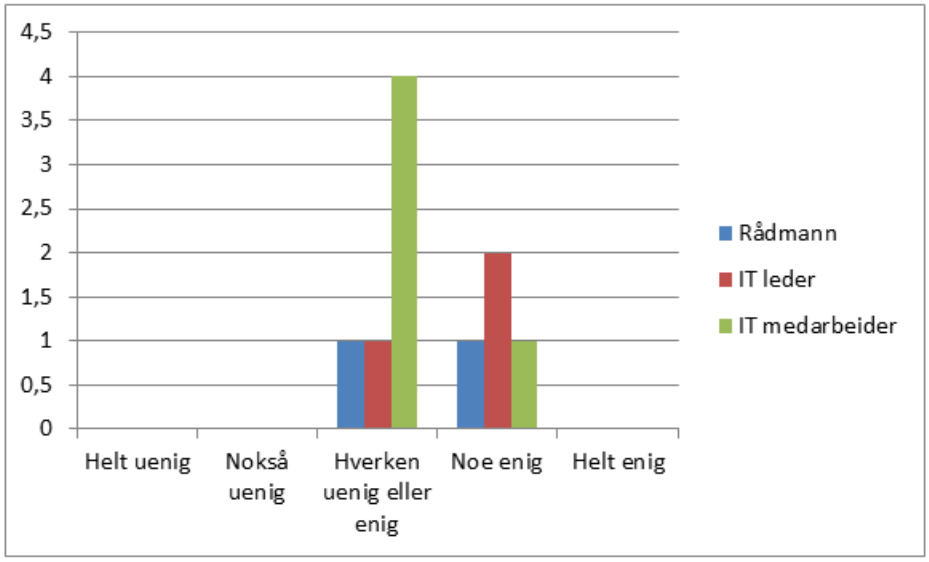
5.2.5 IKT Beredskapsarbeid

På spørsmål om ROS er ikke brukt som grunnlag for IKT beredskapsplan. Med «IKT-beredskap» menes ivaretagelse av alle fylkeskommunens funksjoner, slik at fylkeskommunen kan fungere best mulig som virksomhet, dersom en uønsket hendelse skulle komme til å skje. Her varierer totalbesvarelsen noe, selv om totalbesvarelsen varierer noe ser det ut som hovedtyngden 7/10 (en rådmann, alle IT ledere og tre IT medarbeidere) svarer uenig (i mer eller mindre grad). 3/10 (en rådmann og to IT medarbeidere) svarer «hverken uenig eller enig». Det vil si at de fleste mener risiko og sårbarhetsanalyser er benyttet som grunnlag for IKT beredskapsplan. Resultatene er vist i figur 5.21 under.



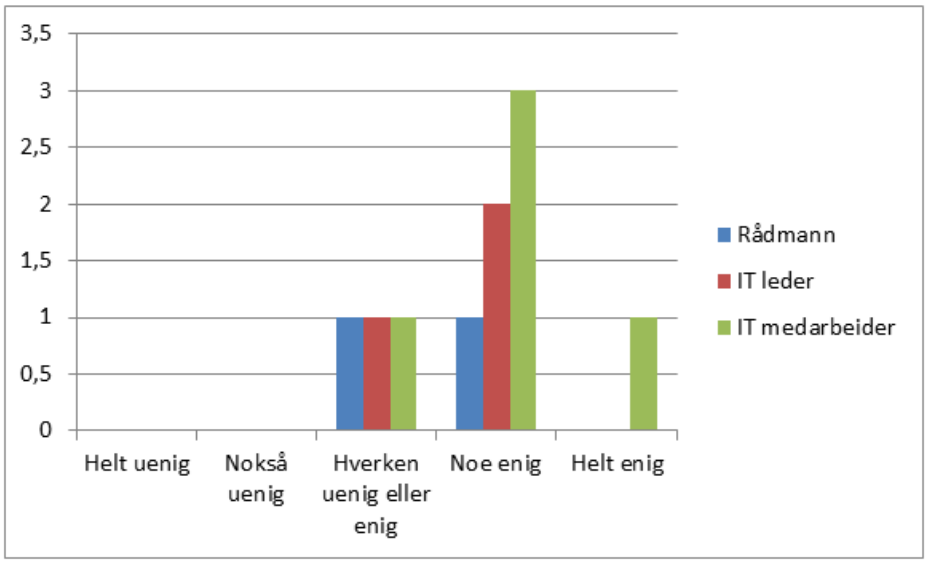
Figur 5.21 ROS er ikke brukt som grunnlag for IKT beredskapsplan.

På spørsmål om det foreligger fullverdig IKT beredskapsplan, varierer totalbesvarelsen noe. 6/10 (en rådmann, en IT leder og fire IT medarbeider) svarer «hverken uenig eller enig» resterende 4/10 (en rådmann, to IT ledere og en IT medarbeider) svarer «noe enig». Resultatene er vist i figur 5.22 under.



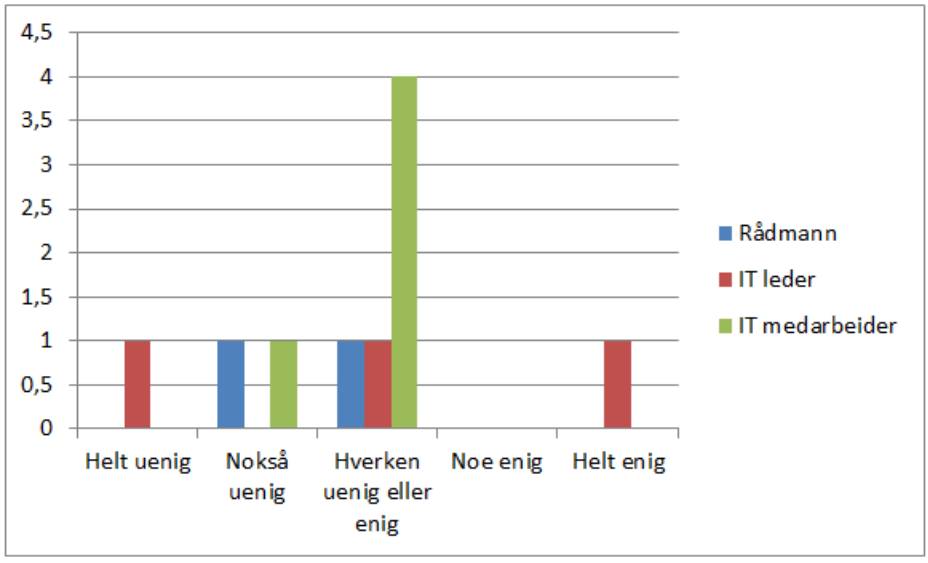
Figur 5.22 Det foreligger fullverdig IKT beredskapsplan.

På spørsmål om det er regelmessig revisjon og oppdatering av IKT beredskapsplanen, varierer totalbesvarelsen ikke så mye. 3/10 (en fra hver stillingsgruppe) svarer «hverken uenig eller enig». Resterende 7/10 (en rådmann, to IT ledere og fire IT medarbeidere) svarer enig (i mer eller mindre grad). Det vil si de fleste respondentene mener det er regelmessig revisjon og oppdatering av planen Resultatene er vist i figur 5.23 under.



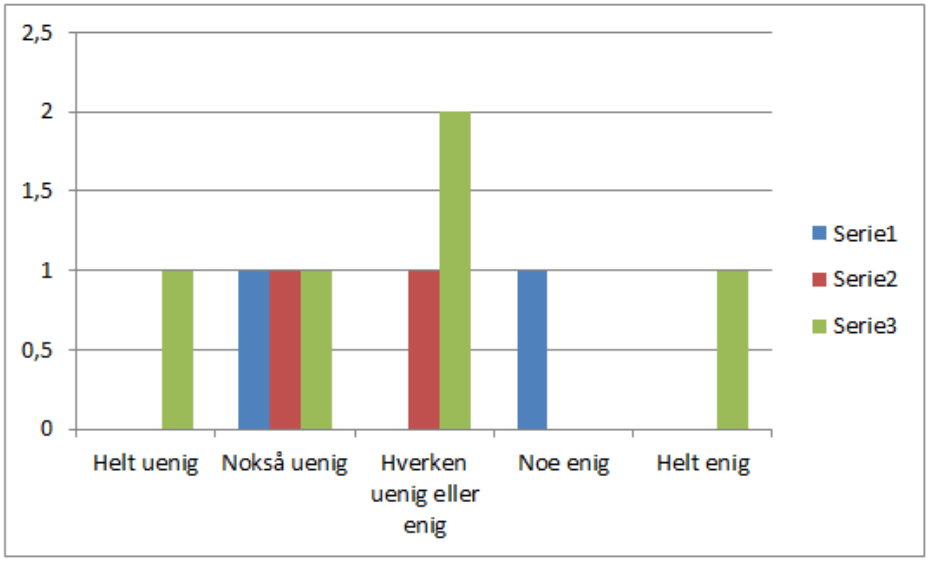
Figur 5.23 Det er regelmessig revisjon og oppdatering av IKT beredskapsplanen.

På spørsmål om det er ikke samsvar med de IKT beredskapsplanene dere har, og annet beredskapsarbeid i fylkeskommunen. Varierer totalbesvarelsen noe, 3/10 (en fra hver stillingsgruppe) er uenig (i mer eller mindre grad). Selv om totalbesvarelsen varierer noe ser det ut som hovedtyngden av respondentene 6/10 (en rådmann, en IT leder og fire IT medarbeidere) svarer «hverken uenig eller enig». Resterende 1/10 (IT leder) svarer «helt enig». Resultatene er vist i figur 5.24 under.



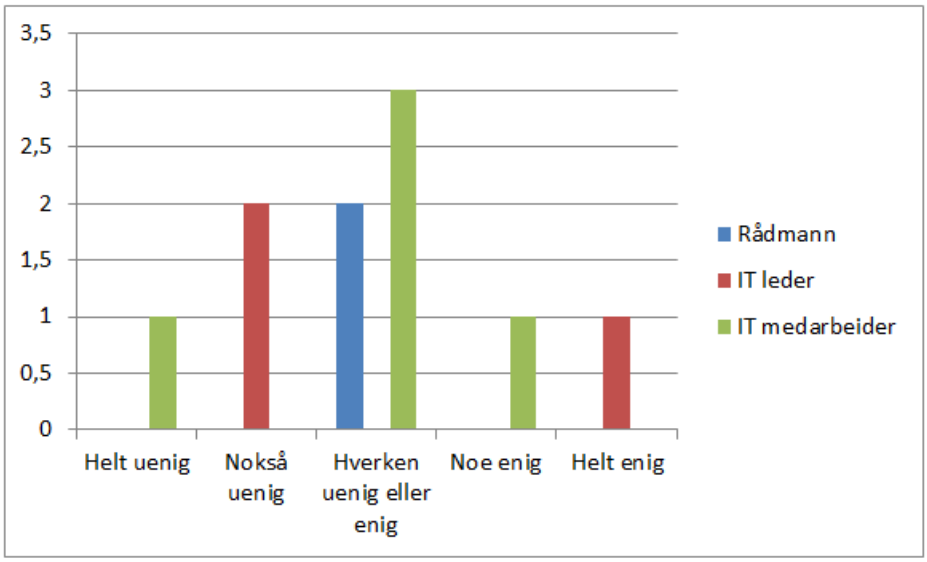
Figur 5.24 Det er ikke samsvar med de IKT beredskapsplanene dere har, og annet beredskapsarbeid i fylkeskommunen?

På spørsmål om det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har kommet til nytte. Her varierer totalbesvarelsen noe, 5/10 (en rådmann, to IT lederne og to IT medarbeidere) svarer uenig (i mer eller mindre grad). 3/10 (en IT leder og to IT medarbeidere) svarer «hverken uenig eller enige». Resterende 2/10 (en rådmann og en IT medarbeider) svarer enig (i mer eller mindre grad). Resultatene er vist i figur 5.25 under.



Figur 5.25 Tidligere hendelser hvor IKT beredskapsplan eller øvelser har kommet til nytte.

På spørsmål om det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har kommet har vært savnet. Her varierer totalbesvarelsen noe, 3/10 (to IT ledere og en IT medarbeider) svarer uenig (i mer eller mindre grad). 5/10 (begge rådmenn, og to IT medarbeidere) svarer «hverken uenig eller enig». Resterende 2/10 (IT leder og IT medarbeider) svarer enig (i mer eller mindre grad). Resultatene er vist i figur 5.26 under.



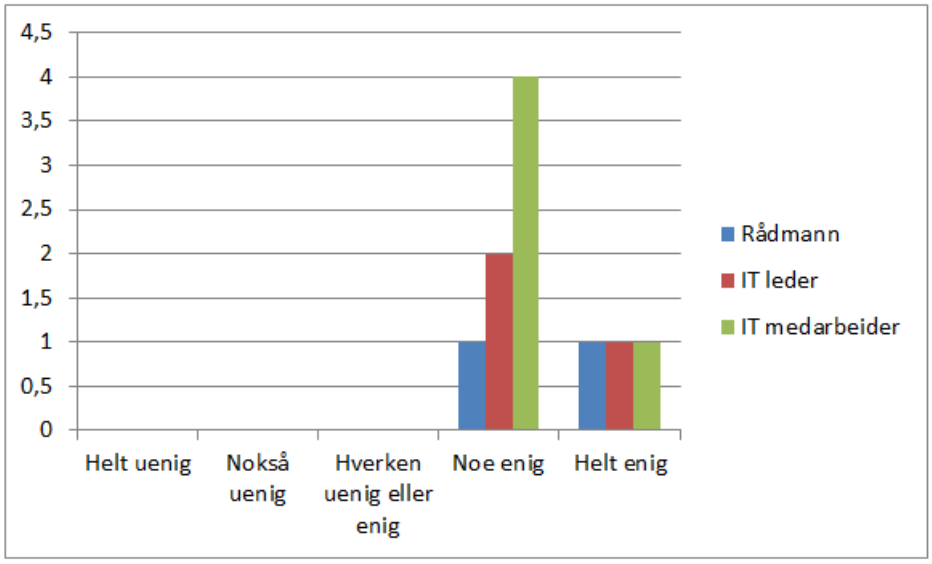
Figur 5.26 Tidligere hendelser hvor IKT beredskapsplan eller øvelser har vært savnet.

På det nevnte åpne spørsmålet, som var etter hvert av spørsmålstemaene der respondenten ble bedt om å utdype eller komme med kommentarer i dette tilfelle fylkeskommunens IKT beredskapsarbeid. Var det ingen av rådmennene som hadde

noen kommentar. En IT leder hadde kommentar « *Vi har enda ikke på plass fullverdig beredskapsplan for å håndtere krise/katastrofe. Dette kommer på plass i løpet av sommer/høst 2013..»* To IT medarbeidere hadde følgende kommentarer *«vi er i ferd med å foreta en større revisjon av beredskapsplan, som ledd i en full revisjon av hele virksomhetens beredskap. Har heldigvis ikke vært særlig bruk for planen hittil.»* Og *«har ikke hatt alvorlige hendelser den tiden jeg har vært her».*

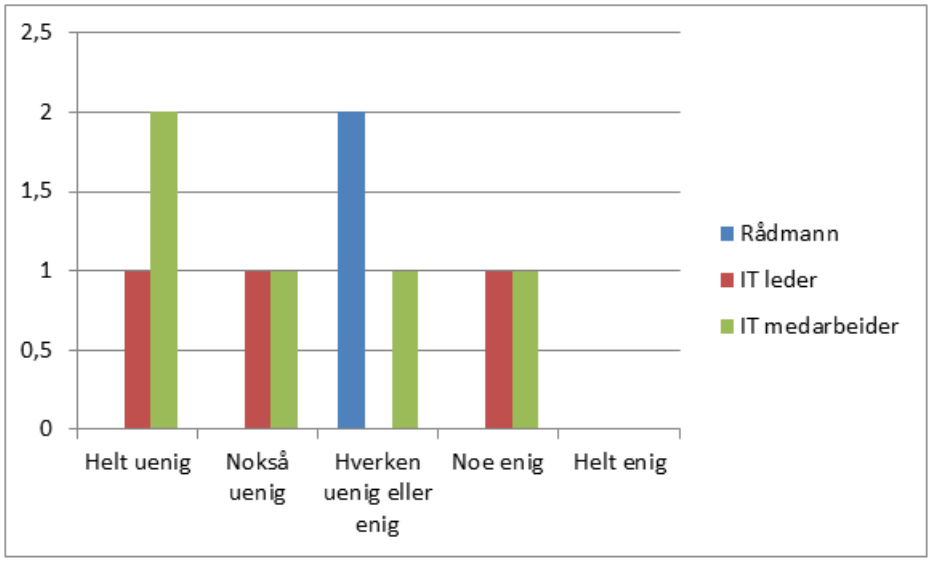
5.2.6 Fylkeskommunens IKT øvelse

På spørsmål om det er ikke øvelse på IKT beredskapsplanen regelmessig, varierer totalbesvarelsen ikke nevneverdig. 10/10 svarer at de er enige (i mere eller mindre grad). Resultatene er vist i figur 5.27 under.



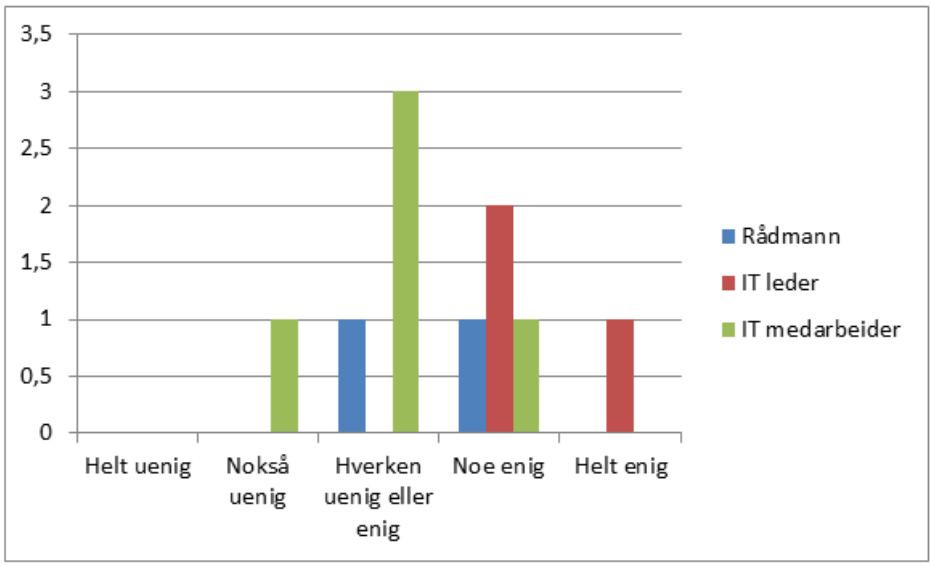
Figur 5.27 Det er ikke øvelse på IKT beredskapsplanen regelmessig.

På spørsmål om det er flere enheter enn ansvarlige for IKT systemene (IT avd.) som er med på øvelse, varierer totalbesvarelsen noe, 5/10 (to IT ledere og tre IT medarbeidere) svarer uenig (i mer eller mindre grad). 2/10 (begge rådmenn og en IT medarbeider) svarer «hverken uenig eller enig». Resterende 2/10 (IT leder og IT medarbeider) svarer «noe enig». Resultatene er vist i figur 5.28 under.



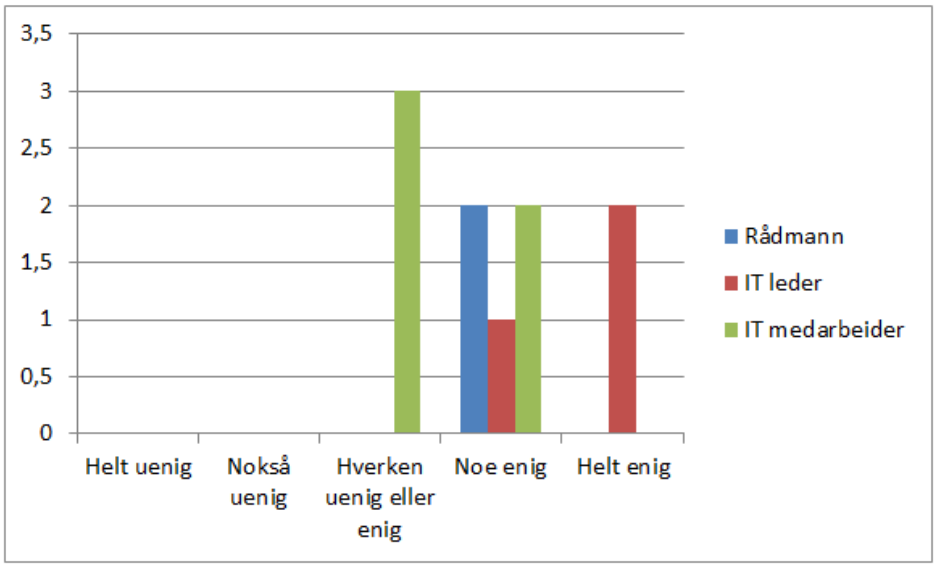
Figur 5.28 Det er flere enheter enn ansvarlige for IKT systemene (IT avd.) som er med på øvelse.

På spørsmål om det er definert hvem som har ansvar for å ta initiativ til IKT øvelser, varierer totalbesvarelsen noe, 1/10 (IT medarbeider) svarer «nokså uenig». 4/10 (en rådmann og fire IT medarbeidere) svarer «hverken uenig eller enig». Resterende 5/10 (en rådmann, alle IT lederne og en IT medarbeider) svarer enig (i mere eller mindre grad). Resultatene er vist i figur 5.29 under.



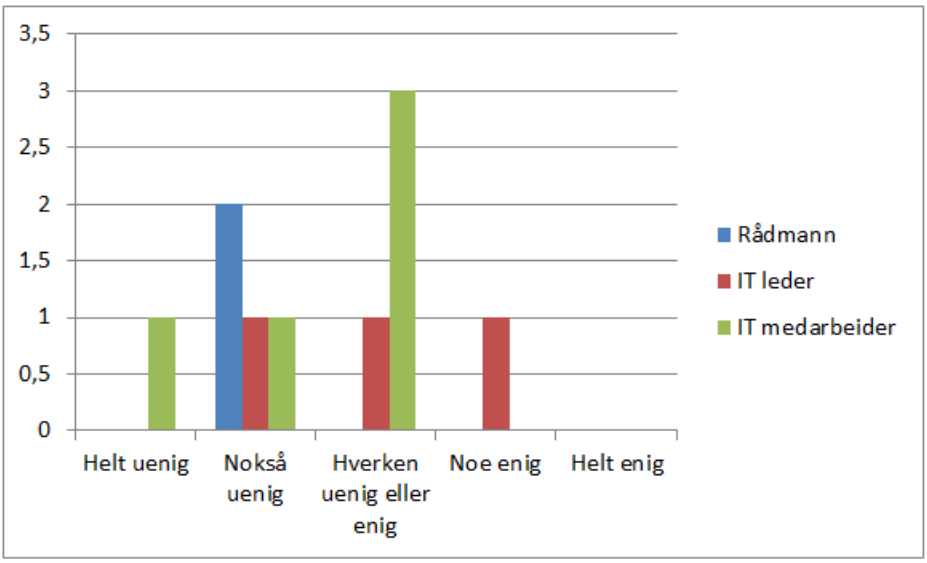
Figur 5.29 Det er definert hvem som har ansvar for å ta initiativ til IKT øvelser.

På spørsmål om tiltak og endringer blir gjort i etterkant av IKT øvelser om det trengs, varierer totalbesvarelsen noe, 3/10 (IT medarbeidere) svarer «hverken uenig eller enig». Selv om totalbesvarelsen varierer noe ser det ut som hovedtyngden av respondentene 7/10 (begge rådmenn, alle IT ledere og to IT medarbeidere) svarer enig (i mer eller mindre grad). Resultatene er vist i figur 5.30 under.



Figur 5.30 Tiltak og endringer blir gjort i etterkant av IKT øvelser om det trengs.

På spørsmål om etter en IKT øvelse er det ikke fokus på positiv læring, her varierer totalbesvarelsen endel. 5/10 (begge rådmenn, en IT leder og to IT medarbeidere) svarer uenig (i mer eller mindre grad). 4/10 (en IT leder og tre IT medarbeidere) svarer «hverken uenig eller enig» resterende 1/10 (IT leder) svarer «noe enig». Resultatene er vist i figur 5.31 under.



Figur 5.31 Etter en IKT øvelse er det ikke fokus på positiv læring.

På det nevnte åpne spørsmålet, som var etter hvert av spørsmålstemaene der respondenten ble bedt om å utdype eller komme med kommentarer i dette tilfelle fylkeskommunens IKT øvelse. Var det ingen av rådmennene som hadde noen kommentar. To IT ledere hadde følgende kommentarer *«Det er systemeier som er ansvarlig for sikkerhet i et IT-system, ikke IT-funksjonen. IT-funksjonen er ansvarlig for*

basis teknisk IT-infrastruktur rundt et system.» Og *«har ikke utført planlagt øvelser enda. Vi har fått erfaringer og "øvelse" i praktisk driftsituasjon, i det vi har hatt sikkerhetshendelser som vi har måttet løse, f.eks. virusangrep, strømbrudd, serverhavari, etc. »*To IT medarbeidere hadde følgende kommentarer *«vi har ikke hatt noen større praktisk øvelse.» Og «har ikke vært gjennomført IKT øvelse (enda). Skjønte ikke begrepet "positiv læring"»*

Sluttspørsmål, var som nevnt tidligere et åpent spørsmål hvor ble respondenten bedt om å utdype eller komme med kommentarer når det gjelder fylkeskommunens IKT sikkerhet og beredskap. Var det ingen av rådmennene som hadde noen kommentar. To IT ledere hadde følgende kommentarer *«For lite fokus hos øverste ledelse. Mener helst at IKT sikkerhet og beredskap er noe IT-avdelingen skal befatte seg med.»* Og *«Det er mye arbeid med å få på plass god IT-beredskap, planer, organisering. Dette er nyttig å jobbe med, spesielt for å heve kvaliteten på virksomheten i det daglige innen IKT-enheten. Ellers vil sikkert bekrefte at det er ulik kunnskap og forståelse for IKT-sikkerhet og beredskap blant medarbeidere i en IKT-enhet. Det må jobbes med å heve kompetanse og forståelse for IKT-sikkerhet i alle ledd.»* En IT medarbeider hadde følgende kommentarer «*Lykke til!»*

6 DRØFTING

Dette kapittelet innbefatter analyse og drøfting av forskjellige teorier sett opp mot mine empiriskefunn. Kapittelet er delt inn i underkapitler med titler som er de ulike temaene i spørreundersøkelsen. Funnene fra empirien vil bli analysert og diskutert, og sammenlignet med funn i Mørketallundersøkelsen™ 2012 .Til slutt vil jeg oppsummere analysevurderingene ved å komme med noen konkrete utfordringer og tiltak for fylkeskommunen.

Som tidligere nevnt i kapittel 1.2 er ikke fylkeskommunen underlagt noe lovverk for behandling av intern IKT sikkerhet og beredskap. Begrepet «internt arbeid med IKT sikkerhet og beredskap» er i denne oppgaven ment som alt arbeid som må til for best mulig å opprettholde fylkeskommunen som virksomhet. Opprettholdelse dersom en uønsket hendelse inntreffer og konsekvensene blir utilgjengelighet av IKT over tid.

Dagens trusselnivå er også gjeldene for fylkeskommunen, på den ene siden er fylkeskommunen en viktig virksomhet for å få det norske samfunnet til å fungere. På den annen side er fylkeskommunen en virksomhet der det ikke er fare for liv og helse, for eksempel ved en uønsket hendelse som resulterer i bortfall av data over tid. Fylkeskommunen er heller ikke et opplagt trusselmål, eller ikke kritisk samfunnsfunksjon. Dette kan være en av grunnene for at myndighetene ikke ser nødvendigheten av lovbestemmelser når det gjelder praktisering av IKT sikkerhet og beredskap internt i fylkeskommunen.

Dersom det hadde foreligget et lovverk, ville det være hensiktsmessig å «måle» resultatene fra min undersøkelse mot gjeldende lover og forskrifter. Siden det ikke finnes, kan det bli en utfordring å «måle» i hvilken grad disse prosessene er ivaretatt og fokusert på. Derfor vil besvarelser fra Mørketallsundersøkelsen være til god nytte sett opp mot funn i oppgavens spørreundersøkelse. Spørreundersøkelsen er delt opp i fem forskjellige temaer som alle omhandler IKT sikkerhet og beredskap, og hvordan dette er ivaretatt i tre fylkeskommuner. Viser til tidligere beskrivelse av spørreundersøkelsen og spørreskjema, samt inndelingen av de fem forskjellige temaene. Dette er grundig beskrevet i kapittel 4.3.3

6.1 Ledelse

Rådmann som ansvarlig for virksomheten ("Jf." Kap.3.1.1) og må ta initiativet til etablering og utvikling av internt IKT lovverk. For å få til et godt lovverk må ledelsen signalisere til de ansatte at de må ta et slikt arbeid på alvor. Selv om ledelsen er drivkraften bak arbeidet, behøver de ikke foreta den detaljerte kontrollen av tiltakene som lovverket omfatter på virksomhetsnivå. *«God virksomhetsarkitektur må balansere mellom det administrative, (ikke tekniske) og det tekniske og operative.»* (Jan T. Bjørnsen 2012, s.6)

Det kan være utfordrende for mange fylkeskommuner å utføre det nødvendige IKT

sikkerhetsarbeidet. Blant annet fordi en ofte mangler kompetanse på dette området. Ved å ha kompetansen på alle nivå innenfor ulike områder, kan dette bidra til at risikoreduserende tiltak iverksettes på et riktig og faglig grunnlag. Dette gir igjen en forutsetning for god styring, og forankring i ledelsen av virksomheten.
For en fylkeskommune vil dette si forankring på flere ledelsesnivåer, fra den øverste administrative ledelse, rådmannsnivået, eller det øverste politiske nivå, fylkestinget.
God styring handler også om økonomi. Reason (1997) mener det er økonomi som bestemmer ulykkesrisikoen ("Jf." Kap.3.1.2). Ser man dette opp mot fylkeskommunen, der det er fylkestinget som behandler forslag til økonomiplan og årsbudsjett, betyr det implisitt at IKT sikkerhetsstyringen må være definert fra rådmann i fylkeskommunen.

Dersom det skulle skje en uønsket hendelse der konsekvens vil være ingen tilgang til datasystemer over lengere tid i fylkeskommunen, vil viktigheten av å ha en god sikkerhetsstyring for best mulig i vareta fylkeskommunen som virksomhet bli ekstremt gjeldende. Dette bør gjenspeile seg i alle prosesser, alt fra årsplaner til budsjettplaner. Ved å budsjettere for sikkerhet vil det bli lettere å følge opp arbeidet, og samtidig ha et bevist forhold til sikkerhet. Ved å gjøre dette, vil effekten av godt innarbeidet sikkerhetsstyring bli gjeldende. Man kan kalle det en type forsvarsverk. I dette tilfellet vil det si på hvilken måte fylkeskommunen tar i bruk forskjellige forsvarsmekanismer, «Defences in depth», myke forsvars barrierer som praktisering, gjennomføring og samarbeid som påvirker IKT sikkerhet og beredskapsarbeidet. Hvis ikke slike forhold ivaretas på en god måte vil disse faktorene være med på å bryte ned forsvarsverket. ("Jf." Kap.3.2.3).

Forsvarsverk i forhold til teknologisk bruk er et aktuelt tema. Vi er en nasjon som tar i bruk mer teknologi, spesielt e-post på mobiltelefoner, og er mer aktive på sosiale medier. Fra datafunn i Mørketallundersøkelsen™ 2012 svarer 88 % at de mottar virksomhetens e-post på mobilen. Og 37 % svarer det foreligger retningslinjer for bruk av privateid utstyr. 53 % svarer at de ikke tillater kunder, samarbeidspartnere eller leverandører tilgang utenfra (via internett) til virksomhetens IT-systemer. ("Jf." Kap.5.1.1).

På spørsmål fra min spørreundersøkelse om det foreligger et fullverdig IKT lovverk fra internt hold, svarer 70 % de er enig i dette. Av respondentene som svarte var alle tre stillingsgrupperingene (rådmenn, IT ledere og IT medarbeidere) representert. De resterende 30 %, en IT ledere og to IT medarbeidere, svarer at de er nokså uenig.("Jf." Figur 5.5). Slik jeg oppfatter det kan se ut som to fylkeskommuner har mer eller mindre et fullverdig lovverk, mens den siste fylkeskommunen som er representert, ikke har det.

Ser man disse besvarelsene opp mot funn fra Mørketallundersøkelsen™ 2012, angående sikker bruk i form av skriftlige utarbeidet retningslinjer og prosedyrer for behandling av informasjon, kom det der fram at over 65 % ikke har retningslinjer når det gjelder sosiale medier, mobiltelefoner eller lagringsmedier ("Jf." Figur 5.1).
Selv om fylkeskommunene kom noe bedre ut, kan det tyde på påstanden som kommer fram i Mørketallundersøkelsen™ 2012 at det ofte mangler retningslinjer stemmer.

En ting er mangel på interne retningslinjer noe annet er forståelse og formidling. Dette er faktorer som påvirker praktisering og gjennomføring av IKT sikkerhet og beredskapsarbeidet. En økt bevissthet av sårbarheter og uønskede hendelser krever åpenhet rundt rapportering (Weick m.fl.1999). ("Jf." Kap.3.1.2)

På bakgrunn av at funn fra Mørketallundersøkelsen™ 2012 er oppgitt i prosent, vil dette også gjelde besvarelser fra mine respondenter.
Et annet spørsmål i min undersøkelse var om IKT lovverket blir ikke overholdt. 40 % (to IT ledere og to IT medarbeidere) svarer «nokså uenig». 40 % (en rådmann, en IT leder og to IT medarbeidere) svarer «hverken uenig eller enig».("Jf." Figur 5.6). Dette vil jeg tro er de samme som svarer de ikke har et fullverdig IKT lovverk. Begrunnelsen for at jeg tror dette er, hvis man ikke har et lovverk kan man heller ikke være «hverken uenig eller enig» om lovverket blir fulgt. 20 % (en rådmann og en IT medarbeider) svarer de er enig. Det vil si 40 % mener de har et IKT lovverk som bli overholdt. På grunn av den negative spørsmålsformen, kan det være en liten sannsynlighet for at spørsmålet er blitt feiltolket av noen. Det som er ganske interessant er at begge rådmennene svarer de har et lovverk, men at det enten blir overholdt eller det er usikkert. Samtidig svarer IT ledere og IT medarbeidere at det blir overholdt.

Ved å vise disse to spørsmålene i en krysstabell, ser man at 70 % svarer bekreftende på det foreligger et fullverdig lovverk (blå ring). 40 % svarer lovverket blir overholdt, samtidig svarer 40 % at de hverken er enig eller uenig i dette (rød ring). Figur 6.1 under.

Det foreligger et fullverdig IKT lovverk fra internt hold	IKT lovverket blir ikke overholdt.					
	Helt uenig	Nokså uenig	Hverken uenig eller enig	Noe enig	Helt enig	Total
Helt uenig	-	-	-	-	-	0
Nokså uenig	-	2	1	-	-	3
Hverken uenig eller enig	-	-	-	-	-	0
Noe enig	-	1	2	-	-	3
Helt enig	-	1	1	2	-	4
Total	0	4	4	2	0	10

Figur 6.1 internt IKT lovverk.

Forsvarsverk kan bidra til å skape en forståelse og bevissthet over hvilke farer man står overfor, og kan gi veiledning i hvordan man kan handle sikkert. I dette tilfellet er det snakk om de myke forsvarsverkene i form av lover og regler, prosedyrer og øvelser. Reason (1997) mener manglende myke forsvarsverker kan være det samme som manglende myke barrierer i denne sammenheng (sveiserostmodellen) ("Jf." Kap.3.2.3). Barrierer som IKT sikkerhet og beredskap, hvordan dette er synliggjort i form av dokumentasjon og hvordan dette er kommunisert, det vil si formidlet og forstått i fylkeskommunen.

Ut i fra dette var det naturlig å stille spørsmål om kvalitetssikring blir overholdt og fulgt opp av interne tilsyn. I min undersøkelse svarer 70 % bekreftende at det finnes en form for kvalitetssikring. ("Jf." Figur 5.7). En inntresang observasjon er begge rådmennene svarer de er «hverken enig eller uenig». Dette kan tyde på en svikt i kommunikasjonen til rådmennene, siden IT ledere svarer noe eller helt enig i at det finnes en form for kvalitetssikring.
Aven m.fl. (2004) påpeker at interne krav er ofte et viktig virkemiddel for å nå fastsatte mål. ("Jf." Kap.3.1.4). Det er IT lederen som må ta initiativ og være pådriver for regler og interne rutiner, og kvalitetssikring for at dette blir fulgt. Slik jeg ser det behøves en det en gjennomgang av lovverket slik at det kan bli enklere å forholde seg til, eller en skarpere metode for å overholde det.

Etter hvert av spørsmålstemaene ble respondentene bedt om å utdype eller komme med

kommentarer, i dette tilfelle fylkeskommunens interne IKT lover og regler. Det var det ingen av rådmennene som hadde noen kommentar. To IT ledere og to IT medarbeidere kommenterte at de hadde slikt lovverk. ("Jf." Kap.5.2.2)

6.2 Sikkerhetsstyring

Sikkerhetsstyring blir omtalt som «*alle tiltak som iverksettes for å oppnå, opprettholde og videreutvikle et sikkerhetsnivå i overensstemmelse med definerte mål*».(Aven m.fl., 2008, s.67) For rådmann handler det om politisk definerte mål, disse skal virkeliggjøres i en administrativ iverksettingsprosess. (Christensen m.fl., 2004) med andre ord rådmannen må ivareta de politiske føringene som er gitt fylkeskommunen, samtidig være øverste leder for administrasjonen i fylkeskommunen. Dette stemmer godt overens med Jacobsen og Thorsvik (2007) som beskriver to perspektiver ("Jf." Kap.3.1.3). Det ene er først og fremst knyttet til hvordan en organisasjon posisjonerer seg når det gjelder sine omgivelser. Det andre retter fokuset mer i mot interne forhold i organisasjonen.

Sikkerhetsstyring i denne sammenheng handler om i hvilken grad IKT beredskapsarbeid er synliggjort og kommunisert, om arbeidet blir vektlagt i internkontrollsystemet. Det handler også om delaktighet i arbeidsoppgaver som omfatter IKT beredskapsarbeidet. Om IKT sikkerhet og beredskap er et ”daglig” tema og formidles til eksterne virksomheter. Det vil si i hvilken grad respondentene er engasjerte, inkluderende og involverte. Og hvordan fylkeskommunen vektlegger praktisering og gjennomføring av arbeidet.

IKT sikkerhet og beredskap blir et mer og mer aktuelt tema, hele virksomheten er helt avhengig av IKT i alle funksjoner. Organiseringen og ansvarsfordelingen er vesentlig for å sikre en effektiv fremdrift og gode resultater av sikkerhetsstyringen.

Aven m.fl.(2004) mener definisjonen av sikkerhetsstyring har to hovedelementer. Det ene er mål (visjoner) og det andre er tiltak (virkemidler). ("Jf." Kap.3.1.3)
Videre skriver han om tiltak for å øke sikkerhetsarbeidet blant annet må sikkerhetsstyringen gripe inn i planlegging og beslutsomhetsaktivitet som til daglig foregår i virksomheten.("Jf." Kap.3.1.4) Et av virkemidlene i så måte vil være internkontroll, det vil si revisjon og kontroll av egne retningslinjer eller prosedyrer. Data fra Mørketallundersøkelsen™ 2012 viser at oppfølging av retningslinjer og prosedyrer rapporteres til ledelsen av 18 % ("Jf." Kap.5.1.2). Det vil si 82 % som ikke rapporterer til ledelsen ved oppfølging.

Aven m.fl. (2004) snakker om involvering eller simulering, som handler om tiltak. For eksempel for å få enkelte mennesker til å gå i en bestemt retning, og der igjennom oppnå ønsket sikkerhet. Slik jeg ser det handler også simulering om forståelse og formidling ("Jf." Kap.3.1.4).
I min undersøkelse har jeg blant annet to spørsmål som omhandler formidling og forståelse av IKT-beredskap. I det ene spørsmålet spørres det om IKT-beredskap er synliggjort og kommunisert til ansatte fra ledelsen. Her varierer besvarelsen en del, 10 % (en IT medarbeider) svarer «helt uenig». 20 % (en rådmann og en IT medarbeider)

svarer «hverken uenig eller enig. ("Jf." Figur 5.8). Selv om besvarelsen varierer noe ser det ut som hovedtyngden av respondentene 70 % (en rådmann, alle IT lederne og tre IT medarbeidere) svarer bekreftende. Det vil si de fleste mener IKT-beredskap er synliggjort og kommunisert fra ledelsen.

I det andre spørsmålet spørres det om IKT sikkerhet og beredskap er synliggjort og kommunisert hos ledelsen. Her svarer hovedtyngden av respondentene 60 % at de er enige. Dette gjelder alle tre IT lederne og tre IT medarbeiderne. 20 % (en rådmann og en IT medarbeider) svarer «nokså uenig». 20 % (en rådmann og en IT medarbeider) svarer «hverken uenig eller enig».("Jf." Figur 5.9).

Det som er ganske interessant er forskjellen på besvarelsen av disse spørsmålene. Det ene omhandler at ansatte mottar og forstår budskapet og det andre omhandler at ledelsen får tilbakemelding fra medarbeidere. Den største forskjellen på besvarelsen er at en rådmann som på det første spørsmålet er «noe enig» og på det neste spørsmålet er «nokså uenig». Jeg tolker det slik at respondenten forstår det slik at ansatte mottar og forstår budskapet, men ledelsen får ikke tilstrekkelig tilbakemelding fra medarbeidere. Videre er det en IT medarbeider som er helt uenig i at ansatte mottar og forstår budskapet samtidig som denne opplever at ledelsen ikke får tilstrekkelig tilbakemelding fra medarbeidere. For å unngå slike ulike oppfattelser skriver Jacobsen og Thorsvik (2007) om ressursbasert perspektiv. ("Jf." Kap.3.1.3)

På spørsmål fra min undersøkelse om IKT beredskapsarbeid vektlegges i internkontrollsystemet, svarer alle IT lederne og to IT medarbeidere «helt enig» og begge rådmenn «noe enig». Derimot er besvarelsen fra IT medarbeidere er noe forskjellige, to svarer «helt enig», en svarer «hverken enig eller uenig», og de to siste svarer «nokså uenig». ("Jf." Figur 5.10). Oppsummer man dette vil det si at 70 % svarer IKT beredskapsarbeid vektlegges i internkontrollsystemet. At flere IT medarbeidere svarer såpas annerledes enn resten av respondentene, kan skyldes at de ikke er involvert i arbeidet, de er kanskje heller ikke informert om innholdet og prosessene i internkontrollsystemet.

Tiltak for bedre IT forståelse og sikkerhet, kan for eksempel være opplæring i sikker bruk av IT og tilhørende retningslinjer. Mørketallundersøkelsen™ 2012 har spurt om nettopp dette. 22 % oppgir der opplæring i sikker bruk av IT regelmessig gjennom ansettelsesperioden. Og 41 % svarer de må undertegne retningslinjer for bruk av IT-systemer. ("Jf." Kap.5.1.2). Igjen viser det forbedringspotensial til å etablere et bedre sikkerhetsfokus.

For å få til dette kreves det god praktisering og godt samarbeid. Jeg ville vite mer om dette. Et nytt spørsmål var derfor om sikkerhet og IKT beredskap er ikke tema på møter, samlinger e.l. Besvarelsen fra respondentene varierer ikke stort. Her svarer 80 % av respondentene benektende. Det vil si en rådmann, alle IT ledere og fire IT medarbeidere mener det er et tema. 20 % (en rådmann og en IT medarbeider) svarer «hverken uenig eller enig». ("Jf." Figur 5.11). Dette kan tyde på at de ikke er involvert eller kanskje heller ikke informert om innholdet i disse møtene.

Videre spør jeg om delaktighet i arbeidsoppgaver som omfatter IKT beredskapsarbeidet. Her varierer ikke besvarelsen vesentlig, 10 % (rådmann) svarer «hverken uenig eller enig». ("Jf." Figur 5.12). Dette kan tyde på at vedkomne ikke er involvert i dette

arbeidet. 90 % av respondentene svarer at de er delaktighet i arbeidsoppgaver som omfatter IKT beredskapsarbeidet.

Ved å vise disse to spørsmålene i en krysstabell, kommer det klart frem at IKT sikkerhet og beredskap er tema på møter, samlinger og lignende. Og de fleste av respondentene er delaktig i IKT beredskapsarbeidet (rød ring). Figur 6.2 under.

Sikkerhet og IKT beredskap er ikke tema på møter, samlinger e.l.	Du er delaktig i arbeidsoppgaver som omfatter IKT beredskapsarbeidet.					
	Helt uenig	Nokså uenig	Hverken uenig eller enig	Noe enig	Helt enig	Total
Helt uenig	-	-	-	-	4	4
Nokså uenig	-	-	-	1	3	4
Hverken uenig eller enig	-	-	1	-	1	2
Noe enig	-	-	-	-	-	0
Helt enig	-	-	-	-	-	0
Total	0	0	1	1	8	**10**

Figur 6.2 sikkerhetsstyring.

«Spesifikke løsninger og tiltak» ("Jf." Kap.3.1.4). Med det mener (Aven m.fl., 2004, s.78) «*Å finne frem til gode løsninger og tiltak handler om kreativitet og nytenkning. Kunnskap, innsikt og erfaring på mange forskjellige områder er en forutsetning for å lykkes*». I min oppgave vil dette bli sett i lys av engasjerte, inkluderende og involverte respondenter.

Neste spørsmål i min undersøkelse er: «Alle» oppfordres til å komme med sine meninger ang. IKT sikkerhetsarbeidet. 70 % (en rådmann og alle tre IT lederne og en IT medarbeider) svarer de er enige. 20 % (en rådmann og en IT medarbeider) svarer «hverken uenig eller enig». 10 % (IT medarbeider) svarer «helt uenig». ("Jf." Figur 5.13). Ut fra disse svarene kan det virke som den ene rådmannen og den ene IT medarbeideren ikke har noen klar oppfattelse av hvorvidt de blir oppfordret til å komme med sine meninger. Samtidig kan det se ut som en IT medarbeider ikke blir inkludert i arbeidet, eller føler det ikke oppfordres til å komme med sine meninger.

På spørsmål om IKT sikkerhet og beredskap er et ”daglig” tema hos dere svarte 10 % (en rådmann) «nokså uenig» og 10 % (en IT medarbeider) svarte «hverken enig eller uenig». 80 % svarer «noe enig». ("Jf." Figur 5.14). I denne besvarelsen var alle tre IT lederne, fire IT medarbeidere og en rådmann enige. Igjen kan det tyde på den ene rådmannen og den ene IT medarbeideren ikke er medvirkende. De er kanskje heller ikke blitt formidlet hvilket fokus IKT sikkerhet og beredskap har i det ”daglige”.

Det siste spørsmålet i temaet sikkerhetsstyring var, sikkerhet og IKT beredskap formidles ikke eksternt til lokasjoner som skole og tannhelse. Her varierer besvarelsen ganske mye, 50 % (en rådmann, en IT leder og tre IT medarbeidere) svarer uenig. 40 %, det vil si den andre rådmann, en IT leder og to IT medarbeidere svarer «hverken uenig eller enig». Den siste IT lederen svarer «noe enig». ("Jf." Figur 5.15). Siden spørsmålet var negativt formet vil det si at 50 % av respondentene mener det blir formidlet sikkerhet og IKT beredskap til eksterne lokasjoner. Den siste 10 % er en IT leder som svarer det ikke blir formidlet sikkerhet og IKT beredskap til lokasjoner som skole og tannhelse.

Etter hvert av spørsmålstemaene ble respondentene bedt om å utdype eller komme med kommentarer, i dette tilfelle til fylkeskommunens sikkerhetsstyring. Det var det ingen av rådmennene som hadde noen kommentar. To IT ledere kommenterte at det var igangsatt arbeid med sikkerhetsstyringen, i form av nedsatt sikkerhetsgruppe, håndbok og rutiner for årlig sikkerhetsrevisjon. Det ble påpekt at sikkerhetsstyring er et kontinuerlig arbeid. ("Jf." Kap.5.2.3)

Selv om det er mye som kan bli bedre, viser Mørketallundersøkelsen™ 2012 til at 82 % oppgir rapportering eller varsling fra egne ansatte som viktigste kilder til å oppdage sikkerhetshendelser ("Jf." Kap.5.1.2). Dette sier noe om sikkerhets fokus i form av delaktighet, og hyppig formidling. Aven m.fl.(2004) skriver om suksessfaktorer for etablering av sikkerhetsstyring, og her blir det lagt vekt på introdusering, lokalisering av ansvar, engasjering fra ledelse, samt fokus på planleggingsfasen og ikke minst oppslutning i å prioritere sikkerhetsarbeidet. Det samme påpeker Jan T. Bjørnsen (2012) som beskriver sikkerhetsstyring som fire sammensatte oppgaver. ("Jf." Kap.3.1.2)

6.3 Risiko- og sårbarhetsanalyse (ROS)

For å lage en ROS analyse må det være definert sårbarheter eller tenkte uønskede hendelser i form av senarioer, det vil si hva som blir konsekvensen av om det skjer og dertil sannsynlighet for at det skjer. ROS er ett sentralt hjelpemiddel for risikostyring, og inngår som en sentral del av risikostyringsprosessen. Slike analyser beskrives som metodiske fremgangsmåter med hensikt å kartlegge og beskrive risiko, for deretter å kunne presentere virksomhetens risikobilde (Aven m.fl.2004) ("Jf." Kap.3.2.2).

Mitt fokus på ROS arbeidet i fylkeskommunen vil dreie seg om utforming av ROS og samarbeid mellom ansvarlige for IKT systemene og ledelsen. Hvorvidt det er gjort ROS med forskjellige senario, ansvarsfordeling og tiltak i form av en handlingsplan når det gjelder de ulike scenarioene. I tillegg ønskte jeg å få svar på om det var regelmessig gjennomføring av ROS arbeidet.

I min undersøkelse ble det spurt om utforming av ROS er et samarbeid mellom ansvarlige for IKT systemene og ledelsen. 60 % svarer «helt enig», deriblant alle tre IT lederne. En rådmann er «hverken uenig eller enig». ("Jf." Figur 5.16). Etter min oppfattelse er det litt underlig at det ikke er samstemthet mellom hva rådmann og IT leder i samme fylkeskommune mener. Selvsagt kan en av dem ha misoppfattet mitt spørsmål, eller så kan dette tyde på dårlig forståelse av samarbeid. Av besvarelsen var det to IT medarbeidere som svarte «hverken uenig eller enig» og «nokså uenig». Slik jeg tolker det kan det være at de ikke er informert eller involvert i prosessen rundt ROS analyser.

Som nevnt tidligere må det ligge en sårbarhet til grunn for å anslå hvilken risiko den enkelte hendelse kan få. Dette gjøres ved å lage forskjellige tenkte senarioer. Mitt spørsmål var om det er gjort ROS med forskjellige senario. Besvarelsen fra respondentene er ganske lik. 70 % svarer «helt enig» og de resterende 30 % svarer «noe enig». ("Jf." Figur 5.17). Litt bemerkelsesverdig var det at begge rådmenn svarer «noe enig» og alle IT ledere svarer «helt enig». Det kan tolkes slik at rådmennene ikke er helt

sikre på om det er gjort ROS med forskjellige senario, eller innholdet i de forskjellige senarioene.

Ser man besvarelsen opp mot Mørketallundersøkelsen™ 2012 oppgir 29 % der at risikovurderinger blir gjort jevnlig i hht etablerte rutiner. Og 45 % oppgir at det gjøres risikovurderinger av og til, avhengig av hvilke løsninger det er snakk om ("Jf." Kap.5.1.2). På dette området kan det virke som fylkeskommunen har litt mer fokus på ROS analyser, selv om ikke alle er involvert eller informert om arbeidet.

Det neste spørsmålet er: Det er ikke gjort en ansvarsfordeling i forhold til de ulike scenarioene i ROS`en. 70 % mener det er gjort en ansvarsfordeling, ved å svare «nokså uenig». De resterende 30 % (en IT leder to IT medarbeidere) mener det ikke er gjort slik fordeling. ("Jf." Figur 5.18).
Aven m.fl.(2004) mener at de som utarbeider ROS analysen bør komme med forslag på tiltak for å redusere risikoen, i tillegg til at tiltakene bør følges opp med vurdering av kostnader sett opp mot gevinsten av dette. Ved å systematisere tiltakene blir det utarbeidet en handlingsplan.

Neste spørsmål omhandler å være best mulig rustet når det gjelder senarioene, og om det er laget en handlingsplan. 80 % svarer de er «noe enig». De resterende besvarelsene var to IT ledere, den ene var «helt enig» og den andre var «hverken uenig eller enig». ("Jf." Figur 5.19). Dette kan tyde på at ikke er helt felles oppfattelse og forståelse av hva den enkelte mener en handlingsplan bør inneholde.

Ved vise disse to spørsmålene i en krysstabell, vil det se slik ut. Det vil si de fleste mener det er laget en handlingsplan og det er gjort en ansvarsfordeling. Rød ring viser tydelig hva de fleste svarer. Figur 6.3 under.

Det er laget en handlingsplan for å være best mulig rustet i forhold til senarioene.	**Det er ikke gjort en ansvars fordeling i forhold til de ulike scenarioene i ROS`en.**					
	Helt uenig	Nokså uenig	Hverken uenig eller enig	Noe enig	Helt enig	Total
Helt uenig	-	-	-	-	-	0
Nokså uenig	-	-	-	-	-	0
Hverken uenig eller enig	-	1	-	-	-	1
Noe enig	-	6	-	1	1	8
Helt enig	-	-	-	-	1	1
Total	0	7	0	1	2	**10**

Figur 6.3 risiko og sårbarhetsanalyse.

Videre ble det spurt: ROS blir ikke gjennomført regelmessig. 50 % svarer «helt uenig, eller nokså uenig». ("Jf." Figur 5.20). Det betyr at ROS blir gjennomført regelmessig. Dette stemmer bra med hva som kom fram av Mørketallundersøkelsen™ 2012 der 66 % av daglige ledere bekrefter at de gjennomfører risikoanalyser ("Jf." Kap.5.1). Det som er bemerkelsesverdig i min undersøkelse er at 40 % svarer «hverken uenig eller enig». Igjen svarer alle tre stillingsgrupperingen forskjellige. Det kan tyde på misforståelse av spørsmålet eller for dårlig formidling og forståelse når det gjelder om det blir gjennomført regelmessig ROS.

Det siste spørsmålet ved hvert tema var som nevnt tidligere åpnet spørsmål, der respondenten ble bedt om å utdype eller komme med kommentarer, i dette tilfelle til

fylkeskommunens ROS. Det var det ingen av rådmennene som hadde noen kommentar. Alle tre IT ledere hadde kommentarer. De påpekte viktigheten av ROS med påfølgende tiltak for alle ledd i fylkeskommunale tjenester. En IT medarbeider hadde følgende kommentarer: «*Det blir gjennomført ROS-analyser ved nye løsninger og konfigurasjonsendringer. Jevnlig (om ikke særlig hyppig) for systemer/løsninger hvor det behandles sensitiv informasjon.*» ("Jf." Kap.5.2.4). Den siste kommentaren stemmer godt overens med hva som kom fram i Mørketallundersøkelsen™ 2012. Av IT-ansvarlige og sikkerhetsansvarlige svarer 84 % at det gjennomføres analyser ved endringer i viktige IT-systemer. Men kun 20 % gjennomfører risikoanalyser hver gang det innføres nye løsninger.("Jf." Kap.5.1.3).

Aven m.fl.(2004) beskriver flere forhold som kan bidra til at styring av sikkerhet blir satt til side, og oppleves som en sekundær prosess som får liten eller ingen betydning i den hele og store styringsprosessen for virksomheten. Ofte er mangel på slik implementering forklart med forhold som mangel på relevant kompetanse, knapphet på tid og ressurser. For best mulig sikre en funksjonell og reell sikkerhetsstyring i fylkeskommunen, vil det være av stor betydning i hvilken grad rådmann og ledergruppen er positive og engasjerte i å prioritere arbeidet. I tillegg er det viktig hvordan de velger å organisere ansvars og oppgavefordelingen. Ut fra besvarelser av min undersøkelse kan det se ut som om de spurte fylkeskommunene ikke er helt i mål. Det ser ut som ROS analyser er noe som arbeides, med men formidling og forståelse av innhold ser ut til å sprike litt.

6.4 IKT beredskapsplan

Målet med IKT beredskapsplan er at den skal legge grunnlag for en effektiv og god krisehåndtering. Det vil si IKT beredskapsplan er å betrakte som et verktøy for krisehåndtering. ROS analyser ligger som grunnlag for etablering av beredskapsplan. For å få en kontinuerlig forbedring av beredskapsarbeidet er det viktig at planverket oppdateres og øves jevnlig. Ut i fra et «bow-tie-diagrammet» ("Jf." Kap.3.2.2) skal risikoanalysen identifisere uønsket hendelser, den skal vise årsakssammenhenger og mulige konsekvenser presentert i et totalt risikobilde.

Mine spørsmål angående tema IKT beredskapsplan omhandlet hvordan planen var bygd opp. Om ROS var brukt som grunnlag for planen, om det foreligger fullverdig plan og om det er regelmessig revisjon og oppdatering av den. Om det er samsvar med IKT beredskapsplanene, og annet beredskapsarbeid i fylkeskommunen. Om det har vært tidligere hendelser hvor IKT beredskapsplaner eller øvelser har kommet til nytte eller vært savnet.

Aven m.fl. (2004) deler sikkerhet og beredskapsarbeidet i to hovedretninger, ("Jf." Kap.3.2).

• Den ene retningen behandler spørsmål om sikkerhet og beredskap implisitt. Ingen har sikkerhet som sin hovedoppgave.

• Den andre retningen behandler spørsmål om sikkerhet og beredskap eksplisitt. Utnevnt personell i en planleggingsgruppe har ansvaret for det som angår sikkerhet og

beredskap.

For å diskutere disse to hovedretninger vil jeg først presentere mine data både fra mørketallsundersøkelsen og min spørreundersøkelse.

Ved funn fra Mørketallundersøkelsen™ 2012 vises det til at av de som har foretatt en risikovurdering har 44 % planer for håndtering av de viktigste informasjons-sikkerhetshendelsene.("Jf." Kap.5.2.5) Det vil si 56 % har ingen plan på håndtering av uønskede hendelser relatert til informasjonssikkerhet. Videre blir det spurt om hvor lang tid det vil ta før det skaper alvorlige konsekvenser for virksomheten dersom de viktigste IT-systemene er ute av drift. 37 % svarer i løpet av 1 time, og 43 % svarer i løpet av 1 dag. ("Jf." Kap.5.1.4). Dette sier noe om avhengighet til IT systemene, og viktigheten av å ha en innøvd beredskapsplan.
Ut i fra besvarelser vedrørende temaet IKT beredskapsplan, der jeg blant annet spør om ROS er ikke brukt som grunnlag for IKT beredskapsplan. Svarer 70 % av respondentene benektende. De resterende 30 % svarer «hverken enig eller uenig» deriblant en rådmann. ("Jf." Figur 5.21). Dette kan igjen tyde på misoppfattelse av spørsmålet som er stilt på denne måten, eller usikkerhet rundt oppbygningen av IKT beredskapsplanen

Jeg ønsker å vite om det foreligger fullverdig IKT beredskapsplan. 60 % svarer «hverken uenig eller enig», og 40 % svarer «noe enig». ("Jf." Figur 5.22). Utfra en slik besvarelse kan en få en oppfattelse av at det er en del arbeid som gjenstår. Det som er interessant ved denne besvarelsen er at to IT ledere svarer «noe enig» og fire IT medarbeidere svarer «hverken uenig eller enig». Her kan det se ut som IT ledere synes de har god nok IKT beredskapsplan, mens IT medarbeidere ikke har den samme oppfattelsen.

På spørsmål om det er regelmessig revisjon og oppdatering av IKT beredskapsplanen svarer 70 % bekreftende at de har det. På dette spørsmålet kan det virke som om det er lik oppfattelse blant de fleste respondentene. Resterende 30 % (en fra hver stillingsgruppering) svarer «hverken uenig eller enig». ("Jf." Figur 5.23). Det går an å spørre seg om det bety at det er en fylkeskommune som ikke har regelmessig revisjon av planene.

En ting er revisjon og oppdatering av egne planer, noe annet er helhetlig beredskapsarbeid for hele fylkeskommunen. På spørsmål om de IKT beredskapsplanene de har og annet beredskapsarbeid i fylkeskommunen ikke samsvarer, svarer 60 % «hverken uenig eller enig». ("Jf." Figur 5.24). Litt spesielt er det at en IT leder svarer «helt enig» siden ingen andre svarer noe bekreftende, årsaken kan være at jeg har stilt spørsmålet på en slik måte. Ut fra besvarelse fra IT medarbeiderne kan det se ut som om det er stor usikkerhet når det gjelder innholdet av den helhetlige beredskapsplanen i fylkeskommunen. Det skal nevnes at kun 30 % (en fra hver stillingsgruppering) svarer bekreftende på at IKT beredskapsplanene samsvarer med annet beredskapsarbeid i fylkeskommunen. En kan stille seg spørsmål om det gjelder en bestemt fylkeskommune.

I et ledd for å forstå nytten av beredskapsplanene spurte jeg om det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har kommet til nytte eller vært savnet. 20 % svarer at dette arbeidet har kommet til nytte. Og 20 % svarer at dette arbeidet har vært savnet ved tidligere hendelser. ("Jf." Figur 5.25). Siden så få ser nytten av

beredskapsplan eller har savnet den ved tidligere anledninger, kan dette skyldes flere forhold som blant annet ulik ansettelsestid, permisjon eller sykefravær. Eller det kan være at fylkeskommunen ikke har hatt noen hendelser hvor det har vært nødvendig med en IKT beredskapsplan.

På begge de overnevnte spørsmålene spriker besvarelsen en del. For å se de ulike besvarelsene i sammenheng (blå ring) vises de i krysstabellen nedenfor. Figur 6.4 under.

Det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har kommet til nytte.	Det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har vært savnet.					
	Helt uenig	Nokså uenig	Hverken uenig eller enig	Noe enig	Helt enig	Total
Helt uenig	1	-	-	-	-	1
Nokså uenig	-	2	2	-	-	4
Hverken uenig eller enig	-	-	2	-	1	3
Noe enig	-	-	1	-	-	1
Helt enig	-	-	-	1	-	1
Total	1	2	5	1	1	10

Figur 6.4 IKT beredskapsplan.

Det ser ut til at å få på plass en beredskapsplan er et aktuelt tema hos de spurte fylkeskommunene. På det åpne spørsmålet, der respondenten ble bedt om å utdype eller komme med kommentarer, sier en IT leder at de har som mål å få ferdig en fullverdig i løpet av sommer/høst 2013. En IT medarbeider sier de er i ferd med å foreta en større revisjon av beredskapsplan, som ledd i en full revisjon av hele virksomhetens beredskap. Det var det ingen av rådmennene som hadde noen kommentar. ("Jf." Kap.5.2.5)

Etter min mening kan det se ut som om fylkeskommunene behandler spørsmål om sikkerhet og beredskap implisitt slik Aven m.fl. (2004) beskriver det. Det vil si ingen har sikkerhet som sin hovedoppgave. Fylkeskommunen er tjent med en mere eksplisitt modell. Der det bør være klare ansvarsfordelinger, klare målsettinger og gode rutiner. For å sikre at formidlingen av budskapet er mottatt og forstått.

6.5 IKT øvelse

For å få til en kontinuerlig forbedring trengs det øvelse og læring. Spesielt når planverket ikke er i bruk ofte, blir det svært viktig med oppdateringer. For best mulig å ha et fungerende planverk er øvelse en nødvendighet.
Momenter som jeg har fokusert på er; om beredskapsplanen blir øvd regelmessig, involvering av ansatte, ansvarsforhold og håndtering av evaluering når det gjelder øvelse. *«Øvelser er en vanlig metode for å forberede ulike grupper i samfunnet på håndteringen av mulige kriser.» (*Fimreite, Lango, m.f., 2011, s.160)

Godt samarbeid, formidling og forståelse av IKT beredskapsarbeidet bidrar til å redusere omfanget av en uønsket hendelse. Som oftest under en krise er en av karakteristikkene at man har liten responstid, jo mer en situasjon er innøvd, jo bedre vil krisen takles. Ved å ha klare ansvarsfordelinger, gode varslingsrutiner og et godt

fungerende planverk står man sterkt rustet om en uønsket hendelse skulle komme til å inntreffe. Reason, (1997) skriver om at lengre perioder uten uønskede hendelser i en virksomhet vil føre til svekket fokus på sikkerhetsarbeidet. Dette fordi fokuset blir sterkere rettet mot produksjonsmålene. ("Jf." Kap.3.2.1)
Et funn fra Mørketallundersøkelsen™ 2012 som viser svekkelse av IKT sikkerheten, er at under 12 % har krav til gjennomføring av systematiske øvelser knyttet til IT-beredskap. ("Jf." Kap.5.1.5). Med så lavt krav kan dette vise dårlig forståelse av hva IKT øvelse og læring gir. I min undersøkelse spør jeg omtrent om det samme: det er ikke øvelse på IKT beredskapsplanen regelmessig. Da svarer 70 % «noe enig» og 30 % svarer «helt enig». ("Jf." Figur 5.27). Her var det en representant fra hver stillingsbetegnelse som svarte. En kan spørre seg om disse var respondenter fra samme fylkeskommune. Det viser at ingen av de spurte fylkeskommunene har regelmessig øvelse på IKT beredskapsplanen.

Fimreite, m.f. (2011) Skriver om betydningen av øvelser. Andre som også påpeker viktigheten av øvelse er (Levin og Klev, 2009) og Direktør i DSB Jon A.Lea ("Jf." Kap.3.2.4). Jacobsen og Thorsvik, (2007) skriver om lærende organisasjoner og systemtenkning. En suksessfaktor vil blant annet være langsiktig strategi og satsing. ("Jf." Kap.3.2.4). Det kan være en utfordring for strategi og langtidsplanleggingen når ledelsen tilsettes på åremål istedenfor permanent tilsettelse. ("Jf." Kap.3.1.1).

Det neste spørsmålet jeg stilte var om det er flere enheter enn ansvarlige for IKT systemene (IT avd.) som er med på øvelse. Her varierer besvarelsen en del, det har nok sammenheng med det neste spørsmålet. Det er bare en IT leder og en IT medarbeider som svarer «noe enig». ("Jf." Figur 5.28). Besvarelsen til begge rådmennene som svarte «hverken uenig eller enig», var ganske interessant. Etter min tolkning kan de ikke ha en rolle i IKT øvelsen eller ikke blitt informert.

Videre spør jeg om det er definert hvem som har ansvar for å ta initiativ til IKT øvelser. Ut fra svarende så kan det se ut som det bare er en IT leder som har en klar oppfattelse av hvem som har et slikt ansvar. To andre IT ledere, en rådmann og en IT medarbeider svarer «noe enig». Det vil si det ikke er en helt klar ansvarsfordeling. 40 % svarer «hverken uenig eller enig». ("Jf." Figur 5.29). Dette var tre IT medarbeidere og en rådmann. Jeg tolker det slik at de ikke vet hvem som har ansvaret eller at de ikke har øvelser. Det er kun en IT medarbeider som svarer «nokså uenig». Det kan forståes slik at de ikke har definert hvem som har ansvar for å ta initiativ til IKT øvelser.

Ved å vise disse to spørsmålene i en krysstabell, vil det være enklere å se variasjon av besvarelsene (blå ring). Figur 6.5 under.

Det er definert hvem som har ansvar for å ta initiativ til IKT øvelser.	Det er flere enheter enn ansvarlige for IKT systemene (IT avd.) som er med på øvelse.					
	Helt uenig	Nokså uenig	Hverken uenig eller enig	Noe enig	Helt enig	Total
Helt uenig	-	-	-	-	-	0
Nokså uenig	-	1	-	-	-	1
Hverken uenig eller enig	2	-	1	1	-	4
Noe enig	1	-	2	1	-	4
Helt enig	-	1	-	-	-	1
Total	3	2	3	2	0	10

Figur 6.5 IKT øvelse.

Jeg spør videre om tiltak og endringer blir gjort i etterkant av IKT øvelser. Her svarer 70 % at de er enig i dette. Tre IT medarbeiderne svarer «hverken uenig eller enig». ("Jf." Figur 5.30). Det kan tyde på at de ikke er involvert etter fått noen informasjon i forhold til om hvilke prosesser det blir gjort i etterkant av IKT øvelser.
Jacobsen og Thorsvik (2007) påpeker at de som sitter nærmest «problemet» er de som oftest ser mulighetene på en mye bedre måte, enn de som sitter høyrere opp i hierarkiet. Ved å skape en kultur for frihetstenkning vil kreativitet og erfaring gi grunnlag for læring. På spørsmål: etter en IKT øvelse er det ikke fokus på positiv læring. Har respondentene en noe ulik oppfattelse av dette. Her svarer begge rådmennene at det er fokus på positiv læring. Tre av IT medarbeiderne svarer «hverken uenig eller enig» i dette. Alle tre IT lederende svarer forskjellig. ("Jf." Figur 5.31). Den sprikende besvarelsen sier en del om hvordan formidling og forståelse av øvelse og læring ivaretas i de spurte fylkeskommunene. Det kan virke som om fylkeskommunene ikke helt følger Jacobsen og Thorsviks teori.

Fimreite, m.f. (2011) viser til forskjellig litratur der det er gjennomgående holdning at øvelse oppfattes som viktig, men får lite fokus. Hovedvekten blir viet til planlegging og utviklingen av planverk. Dette kan stemme godt overens med mine besvarelser.
På spørsmålet der respondenten ble bedt om å utdype eller komme med kommentarer, var det ingen av rådmennene som svarte. En IT leder sier de ikke har utført planlagt øvelser enda, men har fått erfaring i praktisk driftsituasjon. To IT medarbeidere sier de ikke har gjennomført IKT øvelse. ("Jf." Kap.5.2.6).

6.6 Respondentenes opplevelse

Reason (1997) peker på organisasjons motstandsdyktighet eller sårbarhet. Han illustrerer dette gjennom begrepet sikkerhetsrommet, og mener det er tre forhold som påvirker en organisasjons sikkerhetsfokus. Det første omhandler *forpliktelse, ressurser og motivasjon*. Det andre går på *kompetanse*. Det tredje forholdet omhandler *bevissthet omkring sikkerhet*. ("Jf." Kap.3.1.2)

Ser en det første av Reasons tre forhold opp mot funn i spørreundersøkelsen. vil jeg trekke frem at 70 % svarer det foreligger et fullverdig lovverk fra internt hold, og 60 % svarer at lovverket blir overholdt. Og på spørsmålet om det foreligger fullverdig IKT beredskapsplan svarer 60 % «hverken uenig eller enig». Alle respondentene mener det ikke er øvelse på IKT beredskapsplanen regelmessig

Ut fra disse besvarelsene kan det virke som fylkeskommunene har noen mangler når det gjelder bruk av rutiner, utarbeidelse av fullverdig planverk og øvelse av planverk. Siden det ikke er noen form for kontroll eller tilsyn av intern håndtering av IKT, vil det ikke være noe press for å få dette på plass fra eksternt hold. På den andre siden er konsekvensen ved ikke å ha dette på plass ganske liten, sett i lys av hvor sjelden det skjer en uønsket hendelse. Dette kan være med å påvirke hvilket fokus IKT sikkerhet har i fylkeskommunen. Sett i et Reason perspektiv mener jeg at dette vil kunne bevege virksomheten mot økt sårbarhet.

Ser en det andre av Reasons tre forhold opp mot funn i spørreundersøkelsen, kommer det frem at IT medarbeidere er høyere representert, og rådmenn veldig lavt representert når det gjelder å skaffe seg IKT kompetanse. Mørketallundersøkelsen påpeker at daglig leder som øverste ansvarlig, må inneha nok kunnskap om sikkerhet. *«En leder kan delegere oppgaver innen sikkerhet, men ikke ansvaret.»* (Mørketallundersøkelsen™ 2012 s.20)

I min undersøkelse var det to rådmenn som besvarte mine spørsmål og det var ingen av dem som hadde vært i stillingen eller i fylkeskommunen mer enn 8 år. Ingen av dem hadde noen form for utdannelse eller kurs knyttet til IKT sikkerhet og beredskap.
De tre IT ledere som besvarte mine spørsmål, hadde alle vært i stillingen eller i fylkeskommunen mer enn 8 år. Ingen av dem hadde noen form for utdannelse eller langvarige kurs knyttet til IKT sikkerhet og beredskap, en hadde generelle dagskurs. Av IT medarbeidere var det fem stykker (ansatt i forskjellige fylkeskommuner) som besvarte mine spørsmål. Fire har vært i stillingen eller i fylkeskommunen under 8 år, Og en medarbeider har vært lenger enn 8 år. Flere av dem hadde utdannelse i informatikk eller relevante kurs knyttet til IKT sikkerhet og beredskap. På bakgrunn av funnene som ble gjort i spørreundersøkelsen, kan det se ut som de fleste respondentene ikke har vesentlig kunnskap IKT sikkerhet.

Kompetanse innen IKT sikkerhet og beredskap er en viktig forutsetning for å kunne forstå hvilket sikkerhetsnivå fylkeskommunen skal inneha, og hvilke utfordringer som IKT sikkerheten blir møtt med i hverdagen. Aven (2007) påpeker at enhver risikobeskrivelse avhenger av den tilgjengelige kunnskapen og de forutsetningene som gjøres. Dersom ledelsen ved rådmannen ikke innehar noen form for kompetanse, ei heller ikke nødvendig fokus på IKT sikkerhet, kan det være vanskelig for dem som ser IKT sårbarhetene å nå fram med sine argumenter. Selve formidling og forståelse vedrørende IKT sikkerhetsarbeid må komme fra ledelse og ut til medarbeidere er etter min menig meget viktig.

På det tredje forholdet Reason (1997) påpeker, viser funn i spørreundersøkelsen at rådmennene svarer17 av 27 ganger «hverken uenig eller enig». Det var tre ganger begge ga dette svaret samtidig.

Med så høy besvarelse av «hverken uenig eller enig» på spørsmålene tolker jeg det slik på at begge eller i alle fall den ene av rådmennene er svært lite aktiv i IKT sikkerhet og beredskapsarbeidet. På den ene siden kan det også tyde på dårlig samarbeid i form av liten eller ingen formidling, da tenker jeg på praktisering av IKT sikkerhet og beredskapsarbeidet. Mens på den andre siden kan det tyde på at det virker som fylkeskommunen ikke er utsatt for noen synlige trusseler. Jacobsen og Thorsvik (2007) skiller mellom tre vesentlige nivåer for å forsterke samspillet, samordningen og samarbeidet mellom ledelse og de ansatte. Spesielt fremhever de det må være lik forståelse og god ansvarsbevissthet mellom partene ("Jf." Kap.3.1.1).

Der rådmennene svarte 17 ganger «hverken uenig eller enig» svarte IT ledere dette 8 ganger av de 27 spørsmålene. Det var alltid bare en av dem som ga dette svaret. Dette kan tyde på at IT ledere er mer engasjerte og fokuserte på IKT sikkerhet enn rådmennene. På den ene siden er dette selvfølgelig og naturlig siden det er de som har oversikt over sårbarheten i IT systemene, er det de som får «trøkket» ved en uønsket hendelse med konsekvens databortfall over tid. På den andre siden er det urovekkende

at samtlige av IT ledere har vært i sin stilling mer enn 8år, det vil si lengere enn nåværende rådmann. Slik jeg tolker det har det ikke vært vesentlig fokus på, eller kultur for å verifisere at en vet hva som skal gjøres dersom det inntreffer frafall av IKT over tid.

Til sammenligning svarte IT medarbeiderne «hverken uenig eller enig» 21 ganger. Forøvrig var det bare to ganger det var fire stykker som ga dette svaret samtidig, de fleste gangene var det bare en respondent. Dette kan tyde på at ikke alle IT medarbeiderne som ble spurt er særlig engasjerte og fokuserte på IKT sikkerhet.
Det kan være at IT medarbeiderne har større fokus på teknisk sikkerhet som omhandler sikkerhetsmekanismer for å ivareta data, og den tekniske sikkerhet er med stor sannsynlighet ivaretatt hos fylkeskommunene.

For å besvare oppgavens problemstilling var det ikke vesentlig å vite hvilken fylkeskommune respondentene er ansatt ved eller deres navn, derimot var det vesentlig å vite hvilken stilling de innehar, ansettelsestid og kunnskap knyttet til IKT sikkerhet og beredskapsarbeidet. Hensikten med disse spørsmålene var at ved å avdekke hvor lenge og i hvilken type stilling og med hvilken kompetanse respondenten har, vil dette igjen si noe om fokus og holdninger til IKT sikkerhet og beredskapsarbeidet i fylkeskommunen.

På bakgrunn av påpekte sårbarheter i samfunnet generelt, samt økende bruk av IKT. Er det etter min mening verdifullt å vite at alle fylkeskommunens IKT funksjoner er ivaretatt, slik at fylkeskommunen fingrer best mulig som virksomhet dersom en uønsket hendelse skulle oppstå.

Slik jeg ser utfordringer og tiltak for samtlige fylkeskommuner, mener jeg rådmann som har ansvar for sikkerheten må være mer delaktig i prosesser i for hold til IKT sikkerhet. Alle stillingsgrupperingene må påse at informasjon er mottatt og forstått. Klare retningslinjer av ansvar og ansvarsområde. Ferdigstillelse av beredskapsplan, samt hyppigere og regelmessige øvelser.
For å få en bekreftelse på hvor fylkeskommunen står i forhold til å klare å opprettholde virksomheten som virksomhet dersom en uønsket hendelse skulle hende. Vil jeg anbefale å begynne med en øvelse, dette vil gi en pekepinn på hvor IKT sikkerhetsarbeidet er mest sårbart.

7 KONKLUSJON

Problemstillingen som jeg ville besvare i denne oppgaven var:
Hvordan oppfattes IKT sikkerhet og beredskapsarbeidet i tre av landets fylkeskommuner?

Problemstillingen er forsøkt besvart ut fra presentasjon av ulik og relevant teori i kapittel 3, valg av metode i kapittel 4, presentasjon av resultatene i kapittel 5 og sist men ikke minst resultatene i analysen i kapittel 6.

En konkusjon av oppfattelsen av IKT sikkerhets og beredskapsarbeidet i tre fylkeskommuner kan best beskrives som at det må gjøres en jobb for å forbedre dette arbeidet. Gjennom min oppgave har jeg avdekket flere faktorer som kan være årsak til at IKT sikkerhets og beredskapsarbeidet ikke får den oppmerksomhet det fortjener. Samtlige av respondentene som inngår i undersøkelsen mangler formell kompetanse knyttet til fagområdet IKT sikkerhet og beredskapsarbeid.
Ut i fra min undersøkelse har ikke alle fylkeskommunene et internt fullverdig IKT lovverk, det kan også se ut som det gjenstår noe arbeid med formidling og forståelse av dette. Når det gjelder besvarelser angående sikkerhetsstyring hadde ikke respondentene felles forståelse av måten informasjonen ble formidlet på. Derimot var de fleste involvert i arbeidet, det vil igjen si de fleste respondentene er engasjerte i forhold til tematikken IKT beredskap. Tross dette, kan det virke som rådmenn er den gruppen som er mest usikre i arbeidet. Når det gjelder besvarelser fra respondentene angående ROS, er det en del usikkerhet rundt ansvarsfordeling, formidling og full forståelse av arbeidet. Praktisering og gjennomføring av ROS arbeid kan i stor grad virke tilfeldig og lite systematisert da med tanke på når arbeidet skal gjøres, og på hvilken måte.
Ut fra besvarelser angående IKT beredskap kan det virke som usikkerhet rundt oppbygningen og innholdet av IKT beredskapsplanen. Bare tre respondenter (en fra hver stillingsgruppering) svarer bekreftende på at IKT beredskapsplanene samsvarer med annet beredskapsarbeid i fylkeskommunen. Forøvrig ser ut til å få på plass en beredskapsplan er et aktuelt tema hos de spurte fylkeskommunene. Når det gjelder øvelser viser det seg at ingen av fylkeskommunene øver IKT regelmessig. Ut fra besvarelser fra respondensene kan det tyde på usikkerhet når det gjelder ansvarsfordeling både til å ta initiativ til øvelser og hvem som er med på øvelse. Det er også en del usikkerhet av hva som blir gjort i etterkant av en øvelse.

På bakgrunn av at besvarelsene hadde en høy andel av «hverken uenig eller enig» og ingen kommentarer fra noen av rådmennene i de åpne feltene, kan dette tyde på at ledelsen i de tre spurte fylkeskommunene heller ønsker å ha fokus på andre faktorer enn på IKT sikkerhet. Ut ifra besvarelsene fra respondentene er det ikke å ta hardt i med en påstand at hverdagen for ansatte i fylkeskommunen som oftest er ikke preget av et sterkt IKT sikkerhetsfokus. I midlertid er to IT ledere klar over problemet, dette kommer klart frem i sluttspørsmålet i min undersøkelse ("Jf." Kap.5.2.6).

7.1 Veien videre

Det er et bevist valg og ikke å benytte seg av teori angående sikkerhetskultur. Noe som kunne være interessant ved en annen eller en større studie, var å utvide det teoretiske grunnlaget for på denne måten grundigere beskrive alle forhold som påvirker IKT sikkerhetskultur i fylkeskommunen.

8 LITTERATURLISTE

8.1 Dokumenter

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

Aven, T., Boyesen, M. Njå, O., Olsen, K.J., Sandve, K., (2004) *Samfunnssikkerhet*, Universitetsforlaget, Oslo 2004

Aven, T., Røed, W., Wiencke, H.S., (2008) *Risikoanalyse, Prinsipper og metoder, med anvendelser*, Universitetsforlaget, Oslo 2008

Bjørnsen, J.T., (2012) *Slik får du IT-styring og kontroll: handbok for ledere, styremedlemmer og IT-ansvarlige*, Universitetsforlaget, Oslo 2012

Christensen, T., Lægreid P., Roness P.G., Røvik, K.A., (2004) *Organisasjonsteori for offentlig sektor*, Universitetsforlaget, Oslo 2004

Fimreite, A. L., Lango, P., Lægreid, P., Rykkja, L.H., (2011) *Organisering, samfunnssikkerhet og krisehåndtering*, Universitetsforlaget, Oslo 2011

Jacobsen, D. I., (2000) *Hvordan gjennomføre undersøkelser – Innføring i samfunnsvitenskapelig metode*, Høyskoleforlaget, Kristiansand 2000

Jacobsen, D. I., Thorsvik, J., (2007) *Hvordan organisasjoner fungerer*, Fagbokforlaget, Bergen 2007

Klev, R, Levin, M., (2009) *Forandring som praksis. Endringsledelse gjennom læring og Utvikling*, Fagbokforlaget, Bergen 2009

Reason, J., (1997) *Managing the Risks of Organizational Accidents*, Ashgate Publishing Limited, Hampshire 1997

8.2 Internettkilder

DSB, 2012, *Samfunnets sårbarhet over for bort fall av elektronisk kommunikasjon* http://www.dsb.no/Global/Publikasjoner/2012/Rapport/bortfall_elektronisk_kommunikasjon.pdf

DSB, 2012, Samfunnssikkerhet, Nummer 03. september 2012, http://www.haugaland-nett.no/getfile.php/Bilder/Artikkelbilder/DSB_03_Web.pdf

eKommune 2012 - lokal digital agenda, http://www.ks.no/PageFiles/20836/ekommune_2012_revidert_des_2010.pdf

Meld. St. 29 (2011–2012), *Samfunnssikkerhet,* http://www.regjeringen.no/pages/37919076/PDFS/STM201120120029000DDDPDFS.pdf

Mørketallsundersøkelsen - Informasjonssikkerhet og datakriminalitet, http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Mørketallsundersøkelsen/moerketall_2012.pdf

Nasjonal strategi for informasjonssikkerhet, http://www.regjeringen.no/upload/FAD/Vedlegg/IKT-politikk/Nasjonal_strategi_infosikkerhet.pdf

NOU 2000:24, *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet,* http://www.regjeringen.no/Rpub/NOU/20002000/024/PDFA/NOU200020000024000DDDPDFA.pdf

NOU 2003: 18, *Rikets sikkerhet Straffelovkommisjonens delutredning VIII Utredning fra et utvalg under Straffelovkommisjonen oppnevnt ved kongelig resolusjon 21. desember 2001. Avgitt til Justis- og politidepartementet 30. juni 2003,* http://www.regjeringen.no/nb/dep/jd/dok/nouer/2003/nou-2003-18/9/1/2.html?id=371116

NOU 2006:6, *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner,* http://www.regjeringen.no/Rpub/NOU/20062006/006/PDFS/NOU200620060006000DDDPDFS.pdf

Ot.prp. nr. 96 (2005-2006), *Om lov om endringer i lov 25. september 1992 nr. 107 om kommuner og fylkeskommuner m.m (komitémodell, avtalevalg m.m.),* http://www.regjeringen.no/Rpub/OTP/20052006/096/PDFS/OTP200520060096000DDDPDFS.pdf

St.meld. nr. 12 (2006-2007) *Regionale fortrinn – regional framtid,* http://www.regjeringen.no/Rpub/STM/20062007/012/PDFS/STM200620070012000DDDPDFS.pdf

Strategi for samfunnssikkerhet og beredskap i samferdselssektoren, http://www.regjeringen.no/upload/SD/Vedlegg/rapporter_og_planer/N-0546BWEB_sd-strat-samfsik-09.PDF

Weick, K. E., Sutcliffe, K. M., Obstfeld, D., (1999). *Organizing for high reliability: Processes of collective mindfulness Research in Organizational Behavior,* http://www.drillscience.com/DPS/Organizing%20for%20High%20Reliability.pdf

9 VEDLEGG 1 Informasjonsskriv

Masteroppgave-- «*risikostyring og sikkerhetsledelse*»-- Universitetet i Stavanger

SPØRREUNDERSØKELSE - IKT SIKKERHET OG BEREDSKAP

Hei
Mitt navn er Anne Marit Staurheim og arbeider ved Telemark Fylkeskommune i Skien.
Jeg tar en master i «*risikostyring og sikkerhetsledelse*», ved Universitetet i Stavanger.

I forhold til min masteroppgave har jeg plukket ut noen tilfeldige fylkeskommuner som jeg ønsker skal være med i spørreundersøkelse ang. IKT sikkerhet og beredskap.
Som informanter ønsker jeg å ha Rådmann, Leder IT avd. og medarbeidere IT avd.
Spørreundersøkelsen er anonym. Det er ikke noe mål for min masteroppgave å se hvilken fylkeskommune som har eller ikke har god IKT sikkerhet og beredskap.

Hensikten med masteroppgaven er å finne mere ut av hvilket fokus IKT beredskap har i fylkeskommunen generelt, hvilken måte sikkerhetsstyringen blir gjennomført på og hvordan dette påvirker det daglige IKT beredskapsarbeidet i fylkeskommunen.
Med IKT-beredskap menes: hvor godt forberedt er man til å håndtere en uønsket hendelse, som resulterer i bortfall av data med best mulig resultat.
Dette omfatter ivaretagelse av alle fylkeskommunens funksjoner, slik at fylkeskommunen kan fungere best mulig som virksomhet om det skulle skje en uønsket hendelse.

For at oppgaven skal bli en realitet, er jeg avhengig av din hjelp. Ved at du svarer ærlige og oppriktig på spørsmålsundersøkelsen, vil jeg få mulighet til å besvare mine teoretiske spørsmål i oppgaven. Jeg er derfor helt avhengig av din velvilje og positive innstilling til gjennomføring av spørreundersøkelsen.

Selve gjennomføringen av spørreundersøkelsen tar ca.15 min.
Link til spørreundersøkelsen er nederst på siden.

Jeg vil på forhånd takke for din velvilje, at du tar deg tid, og ikke minst for ditt bidrag til spørreundersøkelsen.
Skulle det være behov for å komme i kontakt med meg angående spørsmål i forhold til spørreundersøkelsen, vennligst kontakte meg på:

mobil 90085658 eller pr e-post: anne.staurheim@t-fk.no

Med vennlig hilsen
Anne Marit Staurheim

Svar på spørreundersøkelsen her: (link til undersøkelsen)

10 VEDLEGG 2 Spørreundersøkelsen

Masterstudiet -- risikostyring og sikkerhetsledelse -- Universitetet i Stavanger 24.05.2013

SPØRREUNDERSØKELSE - IKT SIKKERHET OG BEREDSKAP

Spørsmålene vil være rettet mot de faktiske forholdene vedrørende IKT beredskap i fylkeskommunen.

Med IKT-beredskap menes: hvor godt forberedt er man til å håndtere en uønsket hendelse som resulterer i bortfall av data med best mulig resultat. Dette omfatter ivaretagelse av alle fylkeskommunens funksjoner, slik at fylkeskommunen kan fungere best mulig som virksomhet om det skulle skje en uønsket hendelse.

Undersøkelsen er **anonym**, det er ikke noe mål å se hvilken fylkeskommune som har eller ikke har god IKT beredskap.

Selve gjennomføringen av spørreundersøkelsen tar ca.15 min.

Info

Personalia

Jeg ønsker å vite litt om deg og din arbeidssituasjon på de neste spørsmål.

2

Personalia

Hvor lenge har du vært ansatt nåværende stilling?

- ○ Mindre enn 2år
- ○ Fra 2 til 8år
- ○ Mer enn 8år

3

Personalia

Hvor lenge har du vært ansatt i fylkeskommunen?

- ○ Mindre enn 2år
- ○ Fra 2 til 8år
- ○ Mer enn 8år

4

Personalia

Hva er din nåværende stilling?

- ○ Leder (Fylkeskommunen)
- ○ Leder IT avd.
- ○ Medarbeider IT avd.

5

Personalia

Din utdannelse med vitnemål knyttet til IKT sikkerhet og beredskap?

Vennligst fyll ut i boksen over, om du ikke har noen utdannelse med vitnemål svar nei.

Side 1 / 10

6

Personalia

Har du deltatt på relevante kurs ol. knyttet til IKT sikkerhet og beredskap, om ja hvilken?

Vennligst fyll ut i boksen over, over relevante kurs ol. knyttet til IKT sikkerhet og beredskap, hvis du ikke har deltatt svar nei.

Info

Fylkeskommunens interne IKT lover og regler

På de neste spørsmål kommer det påstander knyttet til fylkeskommunens interne lover og regler i forhold til IKT sikkerhet og beredskap. Vennligst fyll ut det som passer best for deg.

8

Fylkeskommunens interne IKT lover og regler

Det foreligger et fullverdig IKT lovverk fra internt hold

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´fullverdig IKT lovverk´ menes lovverk som ivaretar håndtering av for eksempel epost, passord, bruk av bærbar PC og telefon.

9

Fylkeskommunens interne IKT lover og regler

IKT lovverket blir ikke overholdt.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

10

Fylkeskommunens interne lover og regler

Kvalitetssikring av eget arbeid med IKT sikkerhet og beredskap i fylkeskommunen blir fulgt opp av interne tilsyn.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med utførelsen av ´interne tilsyn´ menes for eksempel egen arbeidsgruppe på tvers av fagområder eller personer som ikke direkte er med på utformingen av IKT sikkerhet og beredskaps arbeidet.

Side 2 / 10

11

Fylkeskommunens interne IKT lover og regler

Vennligst utdyp om du har kommentar i forhold til fylkeskommunens interne IKT lover og regler.

Vennligst utdyp i boksen over, om du har kommentar i forhold til fylkeskommunens interne IKT lover og regler, om du ikke har ommentar skriv nei.

Info

Sikkerhetsstyring

På de neste spørsmål kommer det påstander knyttet til fylkeskommunens sikkerhetsstyring i forhold til IKT sikkerhet og beredskap. Vennligst fyll ut det som passer best for deg.

13

Sikkerhetsstyring

IKT-beredskap er synliggjort og kommunisert til ansatte fra ledelsen.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´synliggjort og kommunisert til ansatte´ menes at ansatte mottar og forstår budskapet.

14

Sikkerhetsstyring

IKT sikkerhet og beredskap er synliggjort og kommunisert hos ledelsen.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

´synliggjort og kommunisert hos ledelsen´ menes at ledelsen får tilbakemelding fra medarbeidere.

15

Sikkerhetsstyring

IKT beredskapsarbeid vektlegges i internkontrollsystemet.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Side 3 / 10

16
Sikkerhetsstyring

Sikkerhet og IKT beredskap er ikke tema på møter, samlinger e.l.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

17
Sikkerhetsstyring

Du er delaktig i arbeidsoppgaver som omfatter IKT beredskapsarbeidet.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

18
Sikkerhetsstyring

´Alle´ oppfordres til å komme med sine meninger ang. IKT sikkerhetsarbeidet.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´alle´ menes medarbeidere som arbeider med IKT systemer

19
Sikkerhetsstyring

IKT sikkerhet og beredskap er et "daglig" tema hos dere.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

20
Sikkerhetsstyring

Sikkerhet og IKT beredskap formidles ikke eksternt (til lokasjoner som skole og tannhelse).

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Side 4 / 10

21

Sikkerhetsstyring

Vennligst utdyp om du har kommentar i forhold til Fylkeskommunens sikkerhetsstyring.

Vennligst utdyp i boksen over, om du har kommentar i forhold til fylkeskommunens sikkerhetsstyring, om du ikke har kommentar skriv nei.

Info

Risiko og sårbarhetsanalyser (ROS)

På de neste spørsmål kommer det påstander knyttet til fylkeskommunens risiko og sårbarhetsanalyser (ROS) i forhold til IKT sikkerhet og beredskap. Vennligst fyll ut det som passer best for deg.

23

Risiko og sårbarhetsanalyser (ROS)

Utforming av ROS er et samarbeid mellom ansvarlige for IKT systemene og ledelsen.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

24

Risiko og sårbarhetsanalyser (ROS)

Det er gjort ROS med forskjellige senario.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´forskjellige senario´ menes for eksempel være brann i serverrom, strømbrudd over lengere tid, hærverk eller tyveri i serverrom.

25

Risiko og sårbarhetsanalyser (ROS)

Det er ikke gjort en ansvars fordeling i forhold til de ulike scenarioene i ROS`en.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´ansvars fordeling´ menes ansvar plassert hos enkelte personer hvis noen av scenarioene skulle inntreffe.

26

Risiko og sårbarhetsanalyser (ROS)

Det er laget en handlingsplan for å være best mulig rustet i forhold til senarioene.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´handlingsplan´ menes en plan for best mulig å unngå at noen av senarioene inntreffer.

27

Risiko og sårbarhetsanalyser (ROS)

ROS blir ikke gjennomført regelmessig.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

28

Risiko og sårbarhetsanalyser (ROS)

Vennligst utdyp om du har kommentar i forhold til fylkeskommunens ROS.

Vennligst utdyp i boksen over, om du har kommentar i forhold til fylkeskommunens ROS, om du ikke har kommentar skriv nei.

Info

IKT Beredskapsarbeid

På de neste spørsmål kommer det påstander knyttet til fylkeskommunens IKT beredskapsarbeid. Vennligst fyll ut det som passer best for deg.

30

IKT Beredskapsarbeid

ROS er ikke brukt som grunnlag for IKT beredskapsplan.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Med ´IKT-beredskap´ menes ivaretagelse av alle fylkeskommunens funksjoner, slik at fylkeskommunen kan fungere best mulig som virksomhet, selv om en uønsket hendelse skjedde.

Side 6 / 10

31

IKT Beredskapsarbeid

Det foreligger fullverdig IKT beredskapsplan.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

32

IKT Beredskapsarbeid

Det er regelmessig revisjon og oppdatering av IKT beredskapsplanen.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

33

IKT Beredskapsarbeid

Det er ikke samsvar med de IKT beredskapsplanene dere har, og annet beredskapsarbeid i fylkeskommunen?

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

34

IKT Beredskapsarbeid

Det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har kommet til nytte.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

35

IKT Beredskapsarbeid

Det har vært tidligere hendelser hvor IKT beredskapsplan eller øvelser har vært savnet.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

36

IKT Beredskapsarbeid

Vennligst utdyp om du har kommentar i forhold til fylkeskommunens IKT beredskapsarbeid.

Vennligst utdyp i boksen over, om du har kommentar i forhold til fylkeskommunens IKT beredskapsarbeid, om du ikke har kommentar skriv nei.

Info

Fylkeskommunens IKT øvelse

På de neste spørsmål kommer det påstander knyttet til fylkeskommunens IKT øvelse. Vennligst fyll ut det som passer best for deg.

38

Fylkeskommunens IKT øvelse

Det er ikke øvelse på IKT beredskapsplanen regelmessig.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

39

Fylkeskommunens IKT øvelse

Det er flere enheter enn ansvarlige for IKT systemene (IT avd.) som er med på øvelse.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

40

Fylkeskommunens IKT øvelse

Det er definert hvem som har ansvar for å ta initiativ til IKT øvelser.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

Side 8 / 10

41

Fylkeskommunens IKT øvelse

Tiltak og endringer blir gjort i etterkant av IKT øvelser om det trengs.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

42

Fylkeskommunens IKT øvelse

Etter en IKT øvelse er det ikke fokus på positiv læring.

- Helt uenig
- Nokså uenig
- Hverken uenig eller enig
- Noe enig
- Helt enig

43

Fylkeskommunens IKT øvelse

Vennligst utdyp om du har kommentar i forhold til fylkeskommunens IKT øvelse.

Vennligst utdyp i boksen over om du har kommentar i forhold til Fylkeskommunens IKT øvelse, om du ikke har kommentar skriv nei.

44

Fylkeskommunens IKT sikkerhet og beredskap

Siste spørsmål! Vennligst utdyp om du har kommentar i forhold til fylkeskommunens IKT sikkerhet og beredskap.

Vennligst utdyp i boksen over, om det er noe mer du ønsker å tilføyeom i forhold til fylkeskommunens IKT sikkerhet og beredskaps arbeid, om du ikke har kommentar skriv nei.

Jeg vil på forhånd takke for din velvilje, at du tok deg tid, og ikke minst for ditt bidrag til spørreundersøkelsen.

Skulle det være behov for å komme i kontakt med meg angående spørsmål av spørreundersøkelsen, vennligst kontakte meg på:

mobil 90085658 eller pr e-post: anne.staurheim@t-fk.no

Med vennlig hilsen

Anne Marit Staurheim

Side 9 / 10