Informasjonssikkerhetsstyring i norsk kommunesektor

En case studie

ERLING TOBIAS SKALLEBERG OG MARI CHARLOTTE ÅSTRØM HOLM

VEILEDERE
Geir Inge Hausvik og Carl Erik Moe

Universitetet i Agder, 2021
Fakultet for Samfunnsvitenskap
Institutt for Informasjonssystemer

"There are risks and costs to a program of action — but they are far less than the long-range cost of comfortable inaction"

John F. Kennedy, 35. Presidenten i Amerikas forente stater

Forord

Denne studien markerer slutten på to lærerike år på masterstudiet i informasjonssystemer ved Universitetet i Agder. Lite visste vi at vi kom til å ende opp med en mastergrad i informasjonssystemer, da Erling ferdigstilte sin utdannelse som siviløkonom i 2018, og Mari sin bachelor i folkehelsearbeid samme år. Avhandlingen er del av emnet IS-501, masteroppgave i informasjonssystemer, og er utarbeidet av Erling Tobias Skalleberg og Mari Charlotte Å. Holm, i perioden januar 2021 til juni 2021.

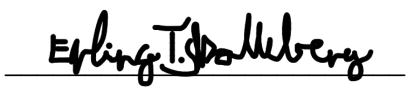
Emnets mål handler om å tilegne seg akademisk spesialisering innenfor et relevant område og bruke teoretisk kunnskap og forskningsmetoder til å svare på et problem. Studien tar for seg informasjonssikkehetsstyring i et utvalg norske kommuner. Informasjonssikkerhet er et høyst aktuelt tema, og nylige angrep mot stat og kommuner viser oss hvor sårbare vi kan være. Dette motiverte oss til å se nærmere på dette.

Først og fremst vil vi takke alle kommunene som har stilt opp og gjort studien mulig. Tusen takk til alle informantene som velvillig har stilt opp med åpent sinn til intervju.

Videre ønsker vi å rette en stor takk til våre veiledere, førsteamanuensis Geir Inge Hausvik og dosent Carl Erik Moe for god veiledning, samtaler og nyttige innspill gjennom studien. Vi vil også rette en takk til førsteamanuensis Peter André Busch som har bidratt med input og veiledning på teoridelen.

Til slutt vil vi takke familie for motivasjon og støtte, samt våre medstudenter for deres oppmuntring og gode vennskap gjennom studietiden. Vi kommer til å savne dere og håper å se dere igjen i arbeidslivet.

Kristiansand, 04.06.2021



Erling Tobias Skalleberg

Mari Charlotte Åstrøm Holm

Sammendrag

Norske kommuner digitaliserer sine tjenester i stadig økende grad, samtidig som trusselbildet fra aktører med ondsinnede intensjoner øker. For å imøtekomme disse truslene og ivareta innbyggernes integritet finnes det ulike styringssystemer for informasjonssikkerhet som enten er anbefalte eller obligatoriske i norsk offentlig sektor. Digitaliseringsdirektoratet peker på at små og mellomstore kommuner har store utfordringer med å praktisere informasjonssikkerhetsstyring.

Gjennom en kvalitativ metode, med 16 semistrukturerte intervjuer i små og mellomstore kommuner i Norge, har vi forsøkt å finne årsaker til, og mulige løsninger på utfordringene kommunene har med informasjonssikkerhetsstyring. Intervjuene varte fra 30-120 minutter, med et gjennomsnitt på 50 minutter. Institusjonell logikk og institusjonelt arbeid som teoretisk linse bidro med en forklaringskraft som ga dypere innsikt og forståelse av årsaker til utfordringene kommunene har med informasjonssikkerhetsstyring. Casestudien vier fokus til et område som er lite forsket på og sådan er et forsøk på å berike eksisterende forskning, samt bidra til både teori og praksis.

Resultatene fra undersøkelsen bekrefter flere av de samme utfordringene som vist i rapporten fra Digitaliseringsdirektoratet, slik som manglende kompetanse og opplæring, utydelige ansvar og roller, begrensede ressurser, samt mangel på revisjoner og kontroll. I tillegg kom vi frem til at spørsmålet rundt eierskap bør adresseres nærmere, særlig spørsmålet hvorvidt man bruker en sentralisert eller desentralisert tilnærming til styring. Studien har bidratt til en dypere innsikt ved å forklare hvordan ulike institusjonelle logikker mellom ansatte sentralt i kommunen og i kommunens virksomheter, slik som skole og oppvekst, opplever gnisninger som kan skape utfordringer i arbeidet med informasjonssikkerhetsstyring.

Institusjonelt arbeid bidro med å forklare hvordan aktører arbeider med å endre institusjonene i virksomhetene slik at man kan støtte informasjonssikkerhetsstyring bedre. Eksempel på slikt arbeid handler om å etablere nettverk som involverer virksomheter og aktører på tvers for å dele erfaringer rundt sikkerhetsarbeidet og som dermed kan øke sikkerhetskulturen. Dette nettverket kunne også bidra til å endre noen av logikkene ute hos virksomhetene til å bedre støtte informasjonssikkerhetsstyring. Andre eksempler på institusjonelt arbeid handler om å definere klare ansvar og roller, sørge for kontroll og revisjoner av informasjonssikkerhetsstyringen slik at den blir forbedret, samt utforme prosedyre for opplæring og utdanning for å skape en bedre sikkerhetskultur. Eierskap kom frem som et viktig funn i studien, hvilket viste seg å fungere best med en desentralisert tilnærming da man involverte aktører på tvers og sørget for at virksomheter i kommunen og deres ledere fikk mer tilknytting til, og bevissthet rundt informasjonssikkerhetsstyring.

Til slutt vil vi påpeke at ressurser kom opp som en av de største utfordringene som hindret arbeidet med informasjonssikkerhetsstyring blant kommunene. Det er viktig at kommuneledelsen er proaktive i sitt syn på informasjonssikkerheten og forstår viktigheten med informasjonssikkerhetsstyring samt hvilken rolle den har i å bevare innbyggernes integritet.

Nøkkelord: Informasjonssikkerhetsstyring (ISS), kommuner, institusjonell logikk, institusjonelt arbeid.

Tabell 1:Begrepsavklaring

Begrep	**Definisjon**
Hjemmel	Et rettslig grunnlag i for eksempel lov, forskrift, avgjørelse i domstol, vedtak eller avtale (Statens innkrevingssentral, u.å).
Informasjonssikkerhet	Bevaring av konfidensialitet, integritet og tilgjengelighet av informasjon (von Solms & van Niekerk, 2013, s. 98).
Informasjonssikkerhetsstyring (ISS)	Etablering og vedlikehold av kontrollmiljøet for å håndtere risikoen knyttet til konfidensialitet, integritet og tilgjengelighet av informasjon og dens støttende prosesser og systemer (Moulton & Coles, 2003, s. 581).
Institusjonell logikk	"... socially constructed, historical patterns of cultural symbols and material practices, assumptions, values and beliefs by which individuals produce and reproduce their material subsistence, organize time and space, and provide meaning to their daily activity" (s.51) (Thornton et al., 2012).
Institusjonelt arbeid	"the sets of practices through which individual and collective actors create, maintain and disrupt the institutions of organizational fields" (Lawrence & Suddaby, 2006, s. 220).
IT-styring	Distribusjon av IT-beslutningsprosessers rettigheter og ansvar blant foretak, interessenter, prosedyrer og mekanismer for å lage og overvåke strategiske beslutninger om IT (Peterson, 2004).
Virksomhetsområde	Kommuner er delt inn i ulike kommunale virksomheter som blant annet helse, oppvekst, skole og teknisk (Statistisk sentralbyrå, 2016). Det er viktig å påpeke at virksomhet som blir henvist til av faglitteratur og forskningsartikler i denne studien omhandler i hovedsak privat sektor og må ikke forveksles med de kommunale virksomhetene.

Innholdsfortegnelse

Liste over figurer

Liste over tabeller

1. Innledning

Et økende antall digitale angrep mot stat og kommuner har blitt rapportert i Norge den siste tiden (Andreas Krantz et al., 2020; Sigrid Gausen et al., 2021; Solbakken, 2020). Samtidig som kommuner digitaliseres i et stadig høyere tempo (Kommunesektorens organisasjon, u.å), blir sårbarheten for digitale trusler større (Departementene, 2019, s. 1) og sensitiv informasjon kan bli tilgjengelige mål for hackere med onde intensjoner (Death, 2017, s. 9). Vinteren 2021 ble Østre Toten kommune utsatt for et dataangrep, hvor alle sikkerhetskopier ble slettet og data kryptert. Datasystemene ble utilgjengelige og sensitiv informasjon kom på avveie (Solbakken, 2020). Digitaliseringsdirektoratet, Nasjonal sikkerhetsmyndighet (NSM) og kommunesektorens organisasjon (KS) sendte raskt ut varsel til norske kommuner etter angrepet om å være oppmerksomme på unormal aktivitet, da det er grunn til å tro at flere dataangrep vil ramme Norge (KS, 2021; Norges Kommunerevisorforbund, 2021; NTB, 2020, 2021) (17.02). I september 2020 ble 10 000 ansatte i syv kommuner i Innlandet utsatt for et alvorlig e-postangrep, der hackere forsøkte å spre virus ved å utgi seg for å være kollegaer av de ansatte i kommunen (Andreas Krantz et al., 2020). Stortinget ble i mars 2021 utsatt for et omfattende dataangrep via deres epost- og kalendersystem, Microsoft Exchange. Dette var en sårbarhet Microsoft først meldte om noen dager i forveien. Det utelukkes ikke at informasjon som ble hentet ut kan bli brukt til spionasje eller til å presse stortingsrepresentanter. Stortingspresidenten omtalte datainnbruddet som et "angrep på demokratiet" (Sigrid Gausen et al., 2021, para.5). Politiets sikkerhetstjeneste (PST) mener at en av de største truslene i 2021 er datasikkerheten, og at utenlandske etterretningstjenester vil bruke store ressurser på å bryte seg inn i norske nettverk og påvirke norske beslutningsprosesser (PST, u.å).

Tall fra Statistisk sentralbyrå viser at en av ti norske kommuner har vært utsatt for dataangrep. 43% av kommunene rapporterte mangel på kompetanse som et problem, og at de sliter med å rekruttere IKT-spesialister (NTB, 2019; Røgeberg, 2019). Under nettangrepet WannaCry i 2017 var det mange organisasjoner som brukte eldre operativsystemer. Selv om tilgjengelige sikkerhetsoppdateringer ble utsendt, ble de ikke tatt i bruk (Bsigroup, 2018, s. 3, 14). Dette angrepet viste viktigheten for organisasjoner om å ha oppdaterte kontroll- og sikkerhetstiltak på plass for å sikre at de er beskyttet mot trusler (Bsigroup, 2018, s. 14). Offentlige organisasjoner ser på informasjonssikkerhet som viktig (Sanders, 2019, para. 2), men en av årsakene til at deler av offentlig sektor fortsatt bruker utdaterte, eldre IT-nettverk, skyldes at IT-budsjetter har vært under press i mange år, og at innovasjonen innenfor IT, overstiger den gjennomsnittlige utskiftningssyklusen for offentlig sektor. I tillegg har flere offentlige organisasjoner ikke en bedriftskultur på plass som muliggjør rask endring (Bsigroup, 2018, s. 14; Sanders, 2019, para.2).

Ettersom kommuner er delt inn i ulike kommunale virksomheter som blant annet helse, oppvekst og teknisk (Statistisk sentralbyrå, 2016, s. 3), besitter og behandler kommunene sensitiv informasjon om deres innbyggere og håndterer mange ulike informasjonssystemer (IS). Å ha et styringssystem for informasjonssikkerheten på plass, er derfor viktig og fører til at man tenker mer helhetlig på arbeidet med informasjonssikkerhet (Digitaliseringsdirektoratet, u.å). Et slikt styringssystem definerer vi i studien som *informasjonssikkerhetsstyring* (ISS), hvilket handler om etablering og vedlikehold av kontrollmiljøet for å håndtere risikoen knyttet til konfidensialitet, integritet og tilgjengelighet av informasjon og dens støttende prosesser og systemer (Moulton & Coles, 2003, s. 581). I de neste avsnittene presenteres motivasjon for studien, valg av problemstilling og forskningsspørsmålene som studien ønsker å besvare.

1.1 Bakgrunn og forskningsspørsmål

Eksempler på angrep de seneste årene gir en indikasjon på norske kommuners sårbarhet. En rapport fra 2020 om informasjonssikkerhet i kommuner, viser at kunnskapsgrunnlaget rundt informasjonssikkerhet ikke er tilstrekkelig i fylkeskommuner og kommuner. Manglende forståelse, kompetanse og sikkerhetskultur legger blant annet grunnlaget for utfordringer med informasjonssikkerhet (Digitaliseringsdirektoratet, 2020, s. 3). Spesielt ble det identifisert utfordringer med styring og kontroll av informasjonssikkerhet i små og mellomstore kommuner. Rapporten viser også at kommunene i liten grad evaluerer, forbedrer eller fornyer styringssystemet for informasjonssikkerhet (Digitaliseringsdirektoratet, 2020, s. 2). Informasjonssikkerhet er et høyst aktuelt tema, og før vi landet de endelige forskningsspørsmålene, undersøkte vi om kommunene faktisk leser dokumenter og holder oversikt over veiledere som finnes om temaet. Etter en samtale med digitaliserings- og utviklingsavdelingen i en kommune, kom det frem at de kun til en viss grad klarer å holde kontroll på styring angående informasjonssikkerhet, og at det er vanskelig og tungvint å følge både anbefalte og obligatoriske standarder (personlig kommunikasjon, 13.01.2021). I tillegg hadde vi korrespondanse med leder for digitaliseringsdirektoratet, e-helsedirektoratet og helseCERT som bekreftet at et styringssystem for informasjonssikkerhet er et område som bør studeres nærmere og som ikke kan regnes som god nok per dags dato (Direktoratet for e-helse, 2019). I e-postkorrespondansen med Digitaliseringsdirektoratet (personlig kommunikasjon, 13.01.2021) skrev de at det hadde vært interessant å intervjue kommunene og undersøke årsakene til utfordringene med å etablere et styringssystem for informasjonssikkerhet.

Vi ønsket i likhet med Digitaliseringsdirektoratet å forstå hvilke utfordringer kommuner møter i arbeidet med ISS. Videre ønsket vi å undersøke hvordan kommuner, som består av ulike virksomheter, personer med forskjellig faglig bakgrunn og kompetanse, har innvirkning på dette arbeidet. Den overordnede problemstillingen er derfor som følger:

> *Hvilke utfordringer står kommuner ovenfor når det gjelder informasjonssikkerhet?*

En rapport fra Digitaliseringsdirektoratet peker på at kommuner har store utfordringer med ISS (Digitaliseringsdirektoratet, 2020, s. 2), men rapporten manglet en forklaring på utfordringene. Vårt mål er derfor å bidra til å forklare utfordringene gjennom følgende forskningsspørsmål:

> *Hva kan forklare utfordringene som kommunene står ovenfor når det gjelder informasjonssikkerhetsstyring?*

I tillegg ønsker vi å bidra med å belyse hvilke tiltak kommunene kan gjøre for å imøtekomme noen av utfordringene basert på litteraturen og kildedata fra intervjuene. Dette leder an til følgende forskningsspørsmål:

> *Hvordan kan kommunene imøtekomme noen av utfordringene med informasjonssikkerhetsstyring?*

For å få svar på forskningsspørsmålene har vi tatt i bruk det teoretiske perspektivet institusjonell logikk og institusjonelt arbeid. Ettersom det er mangel på teori innen ISS (Ada et al., 2009), og tidligere forskning på dette området i hovedsak er deskriptiv og ser primært på rammeverk og praksis (Schinagl & Shahim, 2020), anbefales det å låne teorier fra andre fagfelt slik som sosiologi (Björck, 2004; Schinagl, 2020). Institusjonell logikk har blitt brukt i økende grad innen IS-forskning (Busch, 2018) og kan gi en bedre forståelse av komplekse sosiale realiteter (Berg Johansen & Waldorff, 2015, s. 26). I tillegg er det mangel på studier

som ser på institusjonelt arbeid i tilknytting til praktiske problemstillinger (Lawrence et al., 2013, s. 1030). På bakgrunn av dette kan studien bidra til både teori og praksis.

Forskningsspørsmålene blir besvart gjennom en kvalitativ casestudie hvor vi gjennomførte 16 intervjuer med sikkerhetsansvarlige, personvernombud, rådgivere og kommunedirektører i både små og mellomstore kommuner. Selv om virksomhetsområder som skole, helse og teknisk er berørt av ISS, har vi ikke intervjuet ansatte i disse virksomhetene direkte i vår studie. Studien er også avgrenset til arbeidet med ISS i norske små og mellomstore kommuner.

1.2 Motivasjon for studien

Begge forfatterne er motivert av studiens tidsaktuelle tema og sjansen til å bidra med ny innsikt til et relativt underrepresentert felt innen forskning på informasjonssikkerhet. Vi er motivert av viktigheten informasjonssikkerhet har for å beskytte og ivareta innbyggernes integritet. Det er viktig å påpeke at informasjonssikkerhet ikke er noe som kun omhandler IT-avdelingen eller ledelsen, men som angår oss alle. Vi er også motivert av muligheten til å bidra med forskning som ser forbi det deskriptive og praktiske og tar i bruk teorier som øker forklaringskraften og belyser temaet på en dypere måte. Til slutt ønsker vi å bidra med innsikt som kan brukes av kommuner og etater som kan legge grunnlag for tanker og forbedringer.

1.3 Oppsett og struktur

Resten av studien er strukturert som følger; i kapittel to presenteres de sentrale konseptene informasjonssikkerhet og styring. Kapittel tre består av en litteraturgjennomgang av forskningsfeltet innenfor ISS. Kapittel fire utgjør det teoretiske perspektivet, og i kapittel fem presenteres og begrunnes den anvendte metodikken som er brukt gjennom studien. I kapittel seks gis en oversikt over konteksten og caset i studien. Kapittel syv presenterer resultater og analyse, og i kapittel åtte blir disse diskutert opp mot tidligere forskning. Avslutningsvis konkluderes studien, i tillegg til at implikasjoner for teori og praksis, begrensninger og fremtidig forskning, referanser og vedlegg presenteres.

2. Sentrale konsepter: informasjonssikkerhet og styring

I innledningen ble det pekt på flere hendelser der det hadde skjedd brudd på informasjonssikkerheten i offentlig sektor. I dette kapittelet redegjør vi for de sentrale konseptene, informasjonssikkerhet og styring, samt hvordan disse henger sammen. Begge konseptene blir sett på som viktig for å ivareta virksomhetenes sikkerhet, håndtere risiko og sikre innbyggernes konfidensialitet.

2.1 Informasjonssikkerhet

For å forstå hva ISS kan bidra med, må man definere hva *informasjonssikkerhet* er. Den internasjonale standarden ISO/IEC 27002 (2005), som sitert i (von Solms & van Niekerk, 2013), definerer informasjonssikkerhet som bevaring av konfidensialitet, integritet og tilgjengelighet av informasjon (von Solms & van Niekerk, 2013, s. 98). Informasjonssikkerhet handler om å sikre informasjonsbehandlingen som inngår i oppgaver og tjenester, samt sikre de informasjonssystemene som benyttes. I tillegg handler det om å tilrettelegge prosessene i en virksomhet slik at menneskene som utfører oppgavene kan gjøre dette med tilstrekkelig sikkerhet (Digdir, u.å-c). Overordnet handler det om å sikre at informasjon i alle former:

- Ikke blir kjent for uvedkommende (konfidensialitet)
- Ikke blir endret utilsiktet eller av uvedkommende (integritet)
- Er tilgjengelig ved behov (tilgjengelighet)

Er det brudd på et eller flere av punktene ovenfor, vil det si at det er brudd på informasjonssikkerheten (Digdir, u.å-c).

2.2 Informasjonssikkerhetsstyring

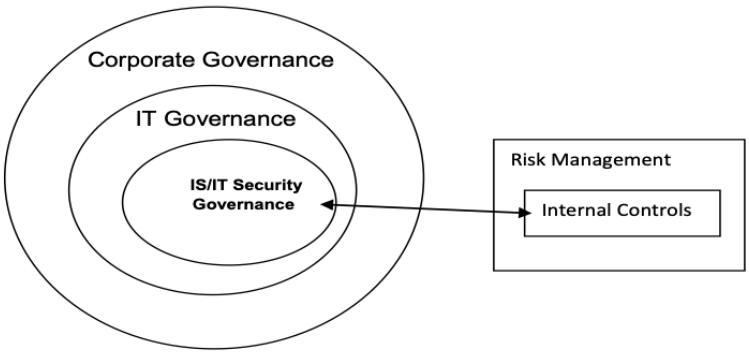
Informasjon, eiendeler og teknologi er tre viktige komponenter som kan skape fortrinn i en organisasjon. Disse står ovenfor stadig mer komplekse og endrede sikkerhetskrav fra interessenter, potensielle trusler og sosio-organisatoriske utfordringer (Stoll, 2013). For å forstå bakgrunnen og sammenhengen mellom informasjonssikkerhet og styring må man først forklare hva styring er.

Styring handler om at medlemmer i en organisasjon vet hva de skal gjøre, hvordan det skal bli gjort, og hvem som skal gjøre det (Whitman & Mattord, 2014, s. 1). Styring kan bli delt inn i flere deler; *eierstyring og selskapsledelse, IT-styring og informasjonssikkerhetsstyring* (Musa, 2018). Eierstyring og selskapsledelse blir definert som "the responsibility of top management for the business value of the organization by implementing good governance that supports alignment between risk management and the organization´s goal" (AlGhamdi et al., 2020, s. 4). IT-styring blir definert som "distribution of IT decision-making rights and responsibilities among different stakeholders in the enterprise, and defines the procedures and mechanisms for making and monitoring strategic IT decisions" (Peterson, 2004, s. 7). ISS er en viktig del av eierstyring og selskapsledelse (Poore, 2005; von Solms & von Solms, 2006) og en viktig bestanddel for å overholde informasjonssikkerheten (Moulton & Coles, 2003, s. 5; Veiga & Eloff, 2007).

Det eksisterer mange definisjoner på ISS, hvor enkelte ser på det som et kontrollmiljø som tar hånd om risiko relatert til informasjonssikkerhet, noen ser på det som en inkorporert del av bedriftsstyring, eller som ledelse, struktur og prosesser (Gashgari et al., 2017, s. 296). Samles flere av definisjonene som finnes om ISS, finner man likheter som støtte fra toppledelse, engasjement, retning, håndtering av risiko og ansvarlighet (AlGhamdi et al., 2020, s. 6).

Mange virksomheter har store strukturelle problemer som for eksempel at informasjonssikkerhetsfunksjonen er plassert innenfor IT, noe som kan føre til at informasjonssikkerhet generelt ikke blir adressert, og som gjør ISS vanskelig eller umulig å iverksette. God styring krever en solid struktur, samarbeid på tvers av virksomheten, velvalgte beregninger, og ressursprioriteringer (Poore, 2005, s. 7).

Å bruke en styringstilnærming til informasjonssikkerhet kan gi et bedre rammeverk for å imøtekomme krav og håndtere risiko i virksomheten. Det kan bidra til mer effektiv kommunikasjon innad i virksomheten og med eksterne interessenter. I tillegg er det med på å etablere klare roller og ansvarsområder (Moulton & Coles, 2003, s. 5). ISS gir virksomheter et rammeverk som er med på å støtte beslutninger for risikobegrensninger og bygge virksomhetens evne til å reagere på interne og eksterne trusler. Samt gjør det mulig å bygge videre på sikkerhetsprogrammet gjennom kontinuerlig tilbakemeldinger fra bunn til topp (Love et al., 2010, s. 17). En sammenheng mellom ISS, IT-styring og eierstyring og selskapsledelse illustreres i Figur 1 (Musa, 2018).



Figur 1: Sammenheng mellom eierstyring og selskapsledelse, IT-styring og bedriftsstyring (Musa, 2018, s. 2).

Modellen viser hvordan internkontroll og risikoledelse er innlemmet som en del av ISS (Musa, 2018, s. 2). Internkontroll henger sammen med informasjonssikkerhet, og er "... leders redskap for å styre risiko på informasjonssikkerhetsområdet" (Digdir, u.å-e). Internkontroll handler om å vedlikeholde og etablere tiltak slik at personopplysninger behandles i samsvar med regelverket (Datatilsynet, u.å). Når virksomheter etablerer god informasjonssikkerhet og internkontroll, sikrer dette at personopplysninger behandles sikkert, lovlig og forsvarlig (Datatilsynet, 2018).

ISS består blant annet av lederskap, organisatoriske strukturer og prosesser som beskytter informasjon. Videre bør de fem grunnleggende resultatene av ISS inkludere (IT Governance Institute, 2006, s. 11-12):

- Strategisk tilpasning av informasjonssikkerhetsstrategi og virksomhetsstrategi som støtter virksomhetens mål.
- Risikostyring ved bruk av de rette tiltakene for å administrere og minimere risiko og redusere potensiell innvirkning på informasjonsressurser til et akseptabelt nivå.
- Ressursledelse ved å unytte informasjonssikkerhetskunnskap og infrastruktur effektivt.
- Ytelsesmåling ved å måle, observere og rapportere ISS-beregninger som sikrer at virksomhetens mål er møtt.
- Verdilevering ved å optimalisere investeringer i informasjonssikkerhet til støtte for virksomhetens mål.

Selv om flere rammeverk og standarder som for eksempel ISO2700-seriene og COBIT gir veiledning på hvordan ISS skal utføres, har forskning funnet svakheter ved bruk av standardene. Blant svakhetene nevnes det at standardene ikke er gode nok for alle områder innenfor ledelse og har mangler i å adressere nye områder (Lidster & Rahman, 2018, s. 2). For å svare på dette har flere forskere prøvd å finne frem til nye rammeverk uten at de har demonstrert at det gir noen verdi. De mangler ofte en veiledning på hvordan man skal implementere ISS, og rammeverk feiler å adressere det dynamiske miljøet som sikkerhet befinner seg i. I tillegg finnes det få gode metoder for å måle styring, tilpasning og hvilken verdi det gir (Lidster & Rahman, 2018, s. 1). Videre mangler standardene et ordentlig rammeverk for implementering og måling av styring (Yassine & Abdelkebir, 2017). Det er viktig at en standard ikke kun regnes som en sjekkliste, men bør brukes som et utgangspunkt og tilpasses den enkelte virksomhet (Siponen & Willison, 2009) (Death, 2017, s. 18), for å sørge for at standarden effektivt sikrer virksomheten (Death, 2017, s. 18).

3. Tidligere forskning

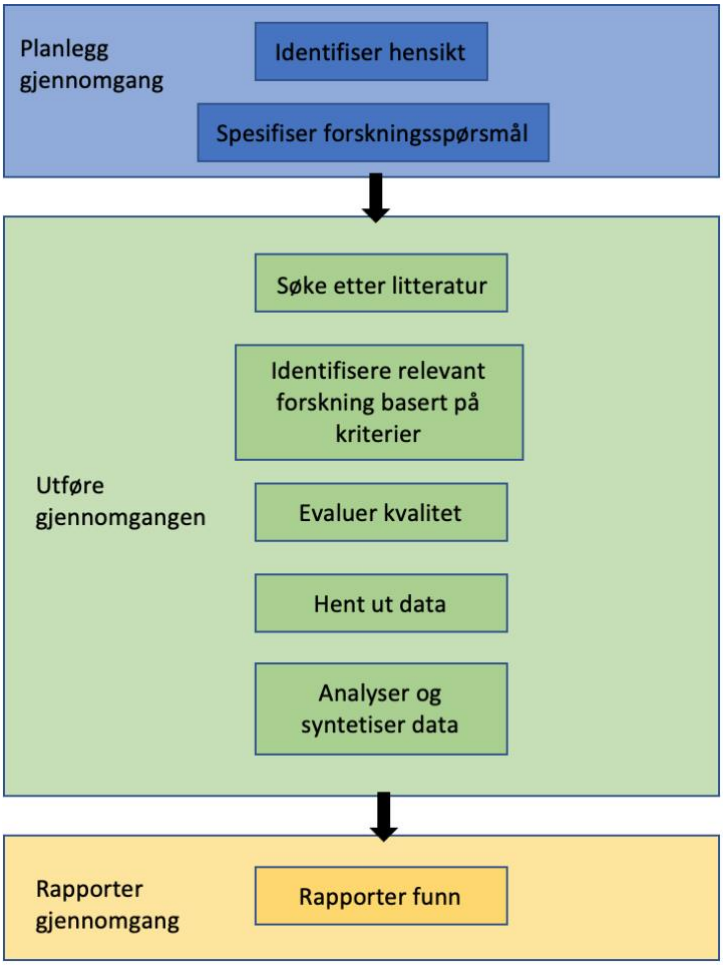
I dette kapittelet har vi via en systematisk litteraturgjennomgang sett på hvordan tidligere forskning har adressert ISS. Dette er med på å skape en dypere forståelse og oversikt over sentrale konsepter som kan bidra med å berike diskusjonen senere i studien. Kapittelet er delt inn i tre deler; (1) planlegge litteraturgjennomgang; (2) utføre litteraturgjennomgang; og (3) rapportere funn.

3.1 Planlegge litteraturgjennomgang

Etter en overordnet redegjørelse for informasjonssikkerhet og styring i avsnittene ovenfor, ønsket vi å gjøre en systematisk litteraturgjennomgang som gikk dypere inn i temaer omkring ISS. Vi spurte oss derfor:

> *"Hvilke tema er adressert i forskning på informasjonssikkerhetsstyring?"*

En gjennomgang av litteraturen er viktig for ethvert akademisk prosjekt og kan hjelpe til med å oppsummere, bidra til teoriskapning, identifisere gap i litteraturen, samt gi forslag til områder for videre forskning (Webster & Watson, 2002, s. 1). En systematisk gjennomgang kan være med på å forbedre kvaliteten og påliteligheten av gjennomgangen (Xiao & Watson, 2019, s. 109). Vi har valgt å ta utgangspunkt i modellen til Xiao og Watson (2019, s. 102-108) for litteraturgjennomgangen, illustrert i Figur 2.



Figur 2: Litteraturgjennomgang prosessen, basert på (Xiao & Watson, 2019, s. 102-108).

3.2 Utføre litteraturgjennomgang

Etter å ha identifisert hensikten og spesifisert forskningsspørsmålet, var neste steg å søke etter litteratur basert på ulike kriterier for å finne informasjon. Et enkelt søk på "information security governance" i Google Scholar ga 1 990 000 treff, i Scopus fikk vi 202 treff, og i Oria 417 treff (søkt 04.03.2021). Disse søkene fungerer for å få en generell oversikt over temaet, men på den andre siden fører det til for mye informasjon, og vi trenger derfor å være mer spesifikke. Et velstrukturert søk i litteraturen var derfor nødvendig. Følgende innhold i Tabell 2 ble identifisert for å bidra til å gi oss nyttig informasjon om spørsmålet vi stilte oss under delkapittel 3.1.

Tabell 2: Søkeord

Søkeord	Synonym
Information security governance	ISO27001

Vi valgte ut to databaser til å fokusere vårt søk på, Oria og Scopus. Vi brukte Boolean operander ved å bruke "OR" og "AND" for å spesifisere søkene (UiA, 2020). Følgende inkluderingskriterier er brukt:

- Kun engelsk språk
- Dokumenttype: kun artikler og konferansebidrag

Vi begrenset ikke søket til et gitt årstall eller "basket of eight" journaler, da dette ikke ga nok resultater for vårt tema. Søket ble derfor relativt åpent.

I Scopus resulterte det i søkestrengen vist i Tabell 3.

Tabell 3: Søkestreng Scopus

Søkestreng
TITLE-ABS-KEY ("information security governance" OR "ISO27001") AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English"))

Søkestrengen gav 219 treff. Disse treffene ble så eksportert til Google regneark i Drive for å få en bedre oversikt over artiklene. Filen inkluderte forfatter/e, abstrakt, årstall, tittel osv. Vi valgte å inkludere konferansebidrag da det fantes mye av dette innenfor ISS feltet.

Videre søkte vi i Oria, som resulterte i 330 treff. I Oria valgte vi å ikke inkludere ISO27001, da dette ga for mange irrelevant artikler. Søkestrengen er vist i Tabell 4.

Tabell 4: Søkestreng Oria

Søkestreng
TITLE-ABS-KEY ("information security governance" AND (LIMIT-TO (DOCTYPE , "cp") OR LIMIT-TO (DOCTYPE , "ar")) AND (LIMIT-TO (LANGUAGE , "English"))

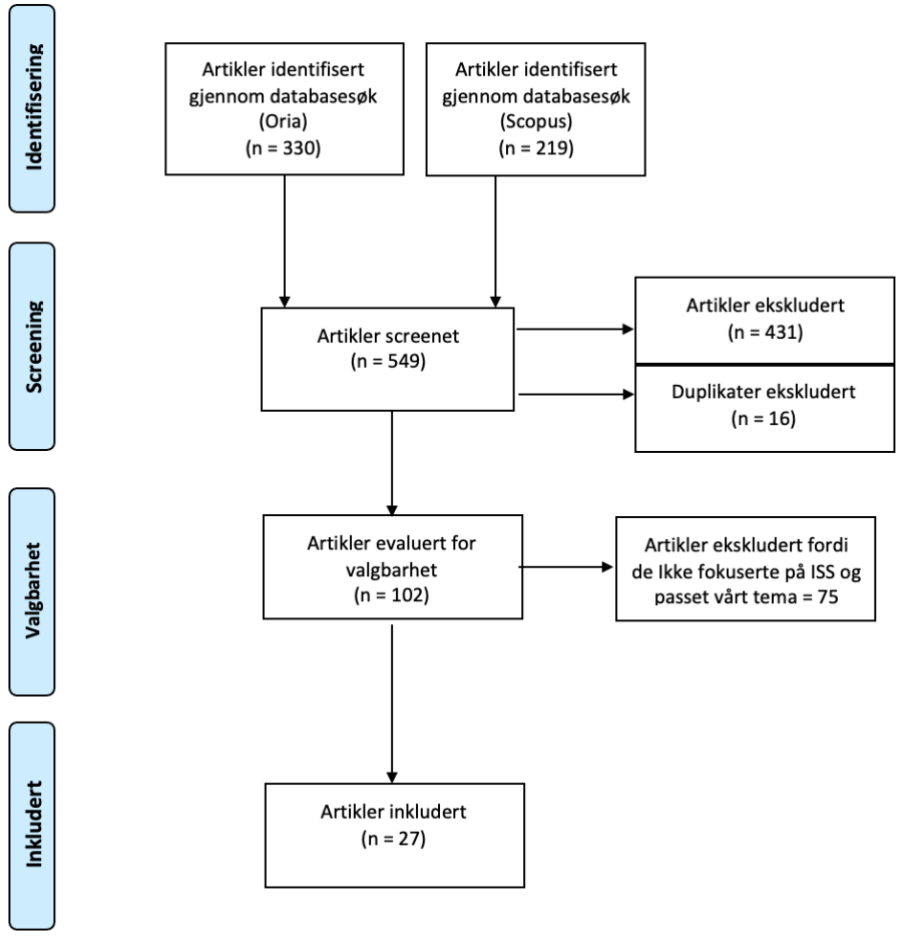
Oria har ikke en eksporteringsfunksjon, noe som gjorde gjennomgangen av artiklene mer uoversiktlig. For å raskt luke ut artikler som ikke var relevante så vi på tittel, abstrakt, om forskningen var relevant for vårt tema, problemstilling og om det gjenspeilet et godt empirisk

grunnlag. Vi ekskluderte derfor artikler ved å bruke spesifikke kriterier slik at det var overkommelig å gjennomføre gjennomgangen av artiklene (Okoli, 2015). Ettersom over 500 artikler er en litt for stor mengde, har vi derfor tatt i bruk ulike ekskluderingskriterier når vi har analysert artiklene, vist i Tabell 5.

Tabell 5: Ekskluderingskriterier

Kriterier	Forklaring
Fagfellevurdert	Ekskluder alle artikler som ikke er fagfellevurdert
Innhold	Ekskluder alle artikler og konferansebidrag som ikke dekker tema og problemstilling

Resultatene fra begge søkene ble gjennomgått systematisk og PRISMA flytdiagram illustrert i Figur 3 visualiserer denne prosessen.



Figur 3: Prisma flytdiagram (Moher et al., 2009)

Vi startet med å gjennomføre en rask gjennomgang av artiklene ved å se på titler og om de var relevante for vårt tema. Etter første screening reduserte vi det ned til 102 artikler. Neste steg var å screene de 102 artiklene ved å lese abstrakt, innledning og konklusjon nøye. Vi ekskluderte da 75 artikler, fordi de ikke fokuserte på ISS og ikke passet vårt tema. Dette var blant annet artikler som omhandlet cybersikkerhet eller kunnskapsdeling. Som vist i figuren ovenfor, gav Oria 330 treff. Av disse var det kun 21 artikler vi så på som relevante. Etter en gjennomgang av 140 artikler, var det flere som ikke inkluderte søkeordene våre i tittel eller

abstrakt, og som var for langt utenfor fokusområde. Av de 21 artiklene var 16 av disse duplikater til de vi allerede hadde screenet i Scopus. Basert på våre søkestrenger og databaser, viser dette at søket i Oria ikke ga oss like mange relevante treff som i Scopus, og at Scopus ga oss mer spesifikke treff. Til slutt endte vi opp med totalt 27 artikler.

3.3 Rapportering av funn

Å strukturere konsepter fra artiklene i en konseptmatrise, jamfør Tabell 6, kan være nyttig for å få en bedre oversikt over viktig og relevante konsepter, samt støtte opp for videre analyse og diskusjon av artiklene (Webster & Watson, 2002, s. 4-6). Konseptene som fremgår av Tabell 6 består av konsepter som vi gjenkjente via en induktiv tilnærming, og som vi forstod som viktig i artiklene. Disse konseptene består av modenhet, sentralisert versus desentralisert styring og støtte fra toppledelsen. De øvrige konseptene er deduktivt basert på deler av Veiga og Eloff (2007) sitt ISS-rammeverk. I konseptmatrisen er rammeverk nevnt to ganger ettersom vi ønsket å undersøke hva rammeverk betyr på generell basis og få et overblikk over ulike rammeverk presentert i litteraturen (markert i grønt). Den andre delen (markert i oransje) relaterer til komponentene i et ISS-rammeverk og går derfor dypere inn i hver komponent og hva disse omfatter. De valgte artiklene er vist i Tabell 6.

Tabell 6: Konseptmatrise

		Konsepter										
		Modenhet	Rammeverk	Komponenter av ISS-rammeverk								
				Lederskap og styring					Retningslinjer	Sikkerhetsprogramledelse		Brukerfokusert sikkerhetsledelse
#	Forfattere			Strategi	Ansvar og roller	Sentralisert vs. desentralisert	Risikostyring	Støtte fra toppledelsen		Revisjoner og kontroll	Etterlevelse	Sikkerhetskultur
1	Yaokumah W.	x		x			x					
2	Asnar Y., Massacci F.						x		x		x	
3	Terence C. C. Tan Anthonie B. Ruighaver Atif Ahmad				x	x				x		
4	Williams P.A.H.		x						x			x
5	Fazlida, M.R ; Said, Jamaliah				x			x	x	x		
6	Mukundan, N R ; Mukundan, N R ; Prakash Sai, L ; Prakash Sai, L				x							
7	Haqaf, Husam ; Koyuncu, Murat				x		x					
8	Slayton, Rebecca		x		x		x					
9	von Solms, Basie ; von Solms, Rossouw				x			x	x		x	
10	Posthumus, Shaun ; von Solms, Rossouw		x	x	x			x				
11	Rebollo, Mellado, Sánchez, Fernández-Medina				x					x		
12	Williams, Susan P ; Hardy, Catherine A ; Holgate, Janine A		x									
13	Gillies, Alan	x			x			x	x		x	
14	Moulton, Rolf ; Coles, Robert S		x									
15	Carcary, Marian ; Renaud, Karen ; McLaughlin, Stephen ; O'Brien, Conor	x	x									
16	Conner, Coviello			x								
17	Veiga, A. Da ; Eloff, J. H. P		x								x	x
18	Heredia H., Merchán V.				x	x				x		
19	Wu S.M., Guo D., Wu Y.C.				x							
20	Gashgari G., Walters R., Wills G.				x							
21	Tan T., Maynard S.B., Ahmad A., Ruighaver T.				x	x				x		
22	Sushma Mishra				x	x						
23	Albuquerque Junior, Antonio Eduardo de ; Santos, Ernani Marques dos			x	x					x		x
24	Von Solms R., Thomson K.-L., Maninjwa P.M.								x			
25	Whitman, Mattord			x								
26	Becker, Moritz Y.								x			
27	Al Ghamdi, S., Win, K. & Vlahu-Gjorgievska, E				x					x		

Fra Tabell 6 har vi identifisert ulike konsepter og funn som har blitt fremhevet som viktige av litteraturen når det gjelder ISS. Disse konseptene og funnene blir diskutert i de kommende avsnittene.

3.3.1 Modenhet

Modenhet gir en indikasjon på hvor godt man har kommet i gang med ISS eller etterlever de målene man har satt seg. Modenheten kan måles ved bruk av indikatorer for å undersøke hvorvidt ISS-retningslinjer, prosedyrer og prinsipper fungerer (AlGhamdi et al., 2020, s. 14).

I tre av artiklene blir modenhet nevnt som en måte for å evaluere og stadfeste hvilket nivå man er i når det gjelder implementering og adopsjon av ISS (Carcary et al., 2016; Gillies, 2011; Yaokumah, 2014, s. 238). Funn viser at virksomheters adopsjon av ISO27001 er tregere enn for andre standarder, og at det er færre som sertifiserer seg innen denne standarden enn andre standarder (Gillies, 2011). For å overkomme dette problemet kan en tilnærming basert på en modenhetsmodell bli brukt, spesielt for mindre virksomheter (Gillies, 2011). Ettersom informasjonssikkerhetslandskapet er i stadig endring, vil virksomheter alltid møte utfordringer med å sikre deres informasjonssystemer. For mange virker det som lett å respondere når det har skjedd et sikkerhetsbrudd ved å adoptere en løsning på det akutte problemet. På en annen side bør man heller være proaktiv og handle strategisk. Det kreves at virksomheter evaluerer deres modenhetsnivå for ISS, slik at man proaktivt kan identifisere problemområder som må tas hånd om (Carcary et al., 2016). For å evaluere modenheten kan man ta i bruk spørreundersøkelser som de relevante interessentene må svare på, og gjennomføre intervjuer for å følge opp hva de svarte i undersøkelsen (Carcary et al., 2016). ISS-modenhetsmodellen har seks nivåer ifølge (Yaokumah, 2014, s. 238):

1) Ikke eksisterende: på dette nivået har ikke virksomheten noen oppfatning om hvilken innvirkning sikkerhetssårbarheter og trusler har på IT-operasjoner, gjør ingen risikoevaluering av prosesser og tenker ikke over behovet for informasjonssikkerhet. I tillegg er ikke ansvarsområder og roller tildelt.

2) Innledende/ad-hoc: på dette nivået ser virksomheten behovet for informasjonssikkerhet og betrakter IT-risiko med en ad-hoc tilnærming. Under dette nivået er uformell risikoevaluering gjort, men ikke målt, og ansvarsområder for IT-sikkerhet er uklart. Dette nivået kan bli betraktet som planleggingsnivået i ISS-implementeringen.

3) Repeterende, men intuitiv: her forstår virksomheten at IT-risiko er viktig, og risikoevalueringer som er umodne er under utvikling. Roller og ansvarsområder er tildelt til en sikkerhetskoordinator uten noen autoritet samtidig som sikkerhetsretningslinjer blir utviklet. Dette nivået kan bli betraktet som en del av planleggingsnivået til ISS.

4) Definerte prosessesser: risikoevalueringer følger definerte prosesser, dokumentert og gjort tilgjengelige for ansatte; programmer for sikkerhetsbevissthet blir promotert av ledelsen; og roller og ansvarsområder er tildelt, men ikke håndhevet.

5) Administrert og målbar: risikoevalueringer følger standard prosedyrer, IT-risikoledelse er ledelsens ansvar, klart tildelt, administrert og håndhevet. Sikkerhetsretningslinjer og praksiser er utviklet og satt på plass. På dette nivået blir sikkerhetsrisiko og konsekvensutredning regelmessig utført og kan bli definert som nesten full implementering av ISS.

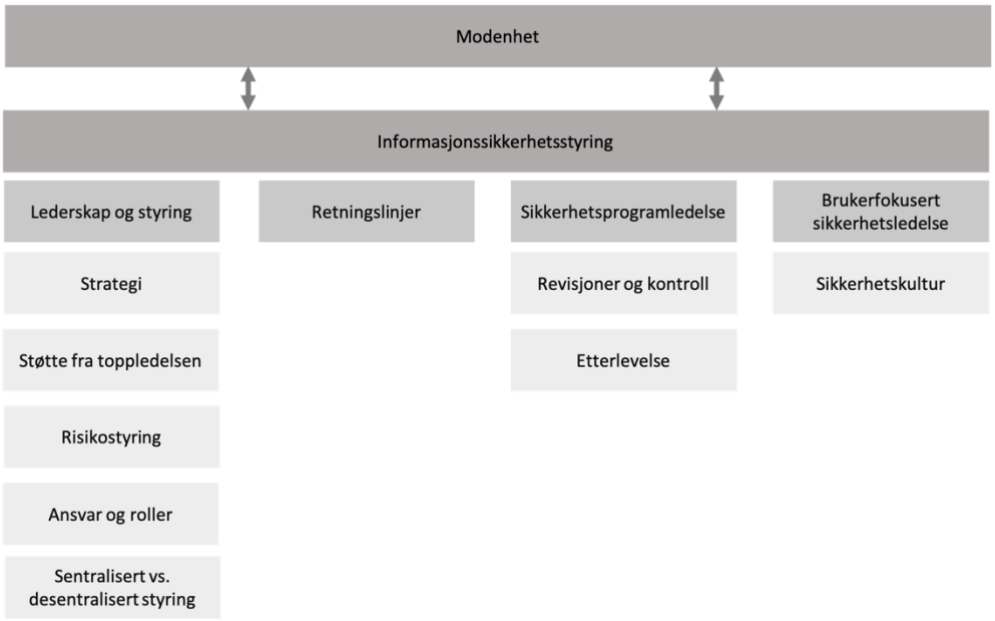
6) Optimalisert: Risikoanalyser er ferdig utviklet og strukturert og prosesser håndhevet; informasjonssikkerhet er et delt ansvarsområde av både virksomhet og IT-ledelsen, og er tilpasset organisasjonens sikkerhets- og virksomhetsmål. I tillegg er informasjon om nye sikkerhetstrusler og sårbarheter samlet inn og regelmessig analysert. Sikkerhet er integrert i applikasjoner når de blir designet og brukere er ansvarlige for å administrere sikkerheten. Dette nivået blir betraktet som fullt implementert ISS.

3.3.2 Rammeverk

Vi ønsket å finne ut hvordan rammeverk har innvirkning på ISS og fant flere artikler som presenterte sine egne rammeverk. Rammeverk er nyttig ettersom det kan brukes som et grunnfundament for ISS og hjelper å sikre de ansattes ansvarlighet for informasjonssikkerheten gjennom et styringsrammeverk (Williams, 2008). Det er et behov for å integrere informasjonssikkerhet i eierstyring og selskapsledelse gjennom ISS-rammeverk for å effektivt styre informasjonssikkerheten i en virksomhet. Rammeverk hjelper også å sikre informasjon gjennom beskyttelse av informasjonssystemer, i henhold til lover og regler, så vel som å forbedre effektiviteten av virksomhetsdriften (Posthumus & von Solms, 2004, s. 645). Selv om rammeverk kan være nyttige for å etablere og evaluere ISS i virksomheter, finnes det lite empiriske bevis som gir innsikt i adopsjon av beste praksis i en organisatorisk omgivelse og i institusjonelle miljøer (Williams et al., 2013). En styringstilnærming til informasjonssikkerhet kan bidra med et rammeverk for å imøtekomme krav og administrere risiko innen virksomheten. Det kan bidra med mer effektiv kommunikasjon med eksterne interessenter, etablere styring, forsvarsroller og ansvar (Moulton & Coles, 2003, s. 584).

Selv om det finnes flere rammeverk for ISS, er de ofte overordnede og teoretiske, uten å gi praktiske tips til hvordan man implementerer og operasjonaliserer disse (Carcary et al., 2016). Risiko som virksomheten møter vil kun bli adressert når et styringsrammeverk er på plass og utstyrt med spesifikke kontroller som ledelsen kan bruke til å dirigere de ansattes oppførsel (Veiga & Eloff, 2007). Et rammeverk gjør det mulig for virksomheten å nå et akseptabelt sikkerhetskulturnivå, og tar hensyn til både tekniske- og prosedyrekontroller, samt det menneskelige aspektet. Det kan bygge på flere standarder og gir virksomheter en forståelse for kravene og en holistisk plan for informasjonssikkerhet. Et rammeverk kombinerer også tekniske, prosedyre og menneskeorienterte komponenter for å ivareta en god nok informasjonssikkerhetskultur og minimere risiko tilknyttet informasjonskapital (Veiga & Eloff, 2007). Det har blitt påpekt at de fleste ISS-rammeverkene som eksisterer er laget for private virksomheter og derfor ikke passer optimalt til offentlige virksomheter (Rebollo et al., 2011). Dette må derfor tas til etterretning ettersom studien fokuserer på det offentlige.

Et rammeverk består av ulike komponenter som er sentrale for ISS. Rammeverkene er ofte omfattende og består av mange ulike komponenter j.fr (Veiga & Eloff, 2007). I dette avsnittet kunne det vært relevant å ta for seg et helt rammeverk, men det vil føre til en altfor omfattende gjennomgang. For å gjøre det mer håndgripelig for denne studien har vi utarbeidet vårt eget rammeverk basert på sentrale komponenter innen ISS. Rammeverket vi presenterer baserer seg på Veiga (2007) og er avgrenset til komponentene som blir mest diskutert blant artiklene fra konseptmatrisen, inkludert modenhet som ble presentert i avsnittet over. Vi har fjernet den tekniske biten som omhandler teknisk beskyttelse og det operasjonelle ettersom dette ikke er et fokus i studien.



Figur 4: Rammeverk for informasjonssikkerhetsstyring basert på (Veiga & Eloff, 2007, s. 363) tilpasset studien

3.3.3 Lederskap og styring

Strategi

Gjennom ISS inkorporeres en strategi for informasjonssikkerhet som adresserer informasjonstrusler via risikovurderinger, strategier for skadebegrensninger og kontroll. Strategien skal være linket til eierstyring og selskapsledelse, samt IT-strategien for å sikre at både kortsiktige og langsiktige mål blir møtt (Veiga & Eloff, 2007, s. 369). Videre kan ISS bli sett på som en del av virksomhetsstyringsstrategien (Conner & Coviello, 2004; Posthumus & von Solms, 2004). For å dirigere en virksomhets informasjonssikkerhetstiltak bør toppledelsen og styret lage retningslinjer for informasjonssikkerheten som viser deres forpliktelse til informasjonssikkerhet, samt støtte til virksomhetens visjon, mål og strategi for informasjonssikkerhet (Posthumus & von Solms, 2004; Whitman & Mattord, 2011). En viktig faktor for å oppnå høyere ISS-modenhet og vellykket implementering, er strategisk tilpasning av både sikkerhet og forretningsvirksomhet (Yaokumah, 2014, s. 239). Det er også viktig at kulturelle og sosiale utfordringer ikke blir separert fra de teknologiske, ettersom problemer med tillit påvirker suksessen til ISS-implementeringen (Williams, 2008, s. 214).

Ansvar og roller

Organisasjonsfaktorer er relatert til ISS og inkluderer formalisering av ansvar og roller (Albuquerque Junior & Santos, 2015). Informasjonssikkerhet må bli vurdert på høyeste nivå i organisasjonen, inkludert styre og toppledelse (Gashgari et al., 2017, s. 295). Deres aktive involvering sikrer at ressursene blir brukt på en sikker måte og at man støtter virksomhetens mål og strategier. En bør også definere klare roller og ansvarsområder, synlig lederskap og sikre at retningslinjer og praksis blir gjort i henhold til lover og regler, samt krav som fremgår av ISS (Gashgari et al., 2017). Å tildele ansvarsområder og ansvarlighet er også en viktig

komponent, og består av at toppledelsen definere tydelige roller og risikoeierskap. Dette vil sikre bedre kommunikasjon internt og eksternt, samt at retningslinjer overholdes (AlGhamdi et al., 2020, s. 6), og er derfor en forutsetning for god informasjonssikkerhet (Mishra, 2015, s. 131).

Sentralisert vs. desentralisert styring

Et omdiskutert spørsmål i litteraturen er hvorvidt en sentralisert eller desentralisert tilnærming til ISS fungerer best. Sentralisert styring kjennetegnes ved at de fleste beslutninger tas av toppledelsen sentralt, mens en desentralisert styring kjennetegnes ved at det er flere personer som er ansvarlig for å ta beslutninger, hvilket krever god sikkerhetsstyring på alle nivåer (Maynard et al., 2018, s. 13, 17). De fleste akademiske artiklene om ISS fremmer en sentralisert tilnærming og dette har blitt kritisert av noen forskere (Maynard et al., 2018, s. 13; Tan et al., 2017, s. 8-9). Problemet med sentralisert beslutningstaking er at det reduserer fleksibiliteten virksomheten har til å tilpasse seg nye retningslinjer og rutiner, samt gjør det vanskeligere å raskt respondere på endringer i sikkerhetsmiljøet (Maynard et al., 2018, s. 13; Tan et al., 2017, s. 8-9).

En bør involvere aktører på det operasjonelle nivået slik at styringspraksisene som fremgår av ISS-rammeverket blir effektivt adressert (Tan et al., 2017, s. 8). En desentralisert sikkerhetsstyring krever god ISS på alle nivåer, og for å kunne imøtekomme dette må styringsstrukturer og prosesser være utviklet og på plass. Dette sikrer at tilstrekkelige sikkerhetsmål og strategier blir utviklet og effektivt kommunisert videre til beslutningstakere (Tan et al., 2010). I tillegg er modne prosesser bedre sikret (Mishra, 2015, s. 131). En desentralisert tilnærming til styring skaper en dynamisk, fleksibel og smidig sikkerhetsstilling. For å oppnå dette, vil det være viktig at nødvendige sikkerhetsstyringsstrukturer og prosessene for hele virksomheten defineres, slik at man sikrer at tilstrekkelig sikkerhetsmål og sikkerhetsstrategier utvikles og kommuniseres effektivt til beslutningstakere (Maynard et al., 2018, s. 77). Det er viktig at organisasjonen effektivt styrer ISS og dens komponenter, retningslinjer og beregninger på en holistisk måte, og former atferd blant aktørene som samsvarer med ISS-modellen (Heredia & Merchán, 2020, s. 468).

Risikostyring

Risikostyring er en viktig og integrert del av ISS (Asnar & Massacci, 2011, s. 2) (som vist i Figur 1) og spiller en rolle ved implementering av standarder slik som ISO/IEC27001 (Haqaf & Koyuncu, 2018, s. 165). På en annen side finnes det en misoppfatning rundt ISS, der usikkerhet som styres med risikostyring i praksis, ikke lar seg gjøre og fører til usikker styring. Ettersom IS ofte består av mange integrerte systemer kan dette føre til økt sårbarhet (Slayton, 2021, s. 81-82), og man er derfor avhengig av gjensidighet og å sikre at alle aktører følger samme agenda (Slayton, 2021, s. 85). Å styre risiko gjennom ISS anbefales derfor å bli gjort via et nettverk ved å involvere alle aktører slik at man skaper en gjensidig interesse (Slayton, 2021, s. 81-82). For å oppnå en høyere modenhet for ISS bør man blant annet fokusere på risikostyring, slik at man kan sikre IT-eiendeler, katastrofegjenoppretting og forretningskontinuitet (Yaokumah, 2014, s. 239). Risikostyring er oppnådd når styret sikrer at risikoevalueringer og skadebegrensninger er integrert i virksomhetens drift for å garantere rask rapportering og respons på utfordringer med sikkerheten (Yaokumah, 2014, s. 239). Risikostyring er med på å minimere risiko og redusere uheldige innvirkninger på informasjonseiendeler til et tilfredsstillende nivå (Yaokumah, 2014, s. 238).

Støtte fra toppledelsen

Støtte fra toppledelsen er nevnt i et flertall av artiklene. Mangel på støtte fra toppledelsen er en barriere når det gjelder adopsjon av ISO2700-serien og standarder (Gillies, 2011). Toppledelsen har et ansvar med å delegere styring og ansvarsområder for å sikre at alle informasjonsaktiva er tilstrekkelig sikret, samt at forsiktighet og aktsomhet er tatt for å opprettholde en slik sikkerhet (von Solms & von Solms, 2004, s. 372). ISS kan kun oppnås så lenge informasjonssikkerhetstiltak kommuniseres tydelig fra toppledelsen til lavere nivåer i virksomheten (Fazlida & Said, 2015, s. 247). Støtte fra toppledelsen spiller en viktig rolle for å lykkes med organisasjonens arbeid med informasjonssikkerhet. Når dette er etablert kan rammeverket for ISS bli brukt for å demonstrere hvordan ledelsen på utøvende nivå skal uttrykke sin støtte til informasjonssikkerhet i virksomheten (Posthumus & von Solms, 2004).

3.3.4 Retningslinjer

Retningslinjer er blant annet betegnet som selve basisen for all beste praksis innen ISS (Becker, 2007). Retningslinjer bør være definert som minimum standard for å overholde informasjonssikkerheten i en virksomhet, men dette alene, er ikke godt nok (Williams, 2008, s. 209). Uklare sikkerhetsretningslinjer er et hinder for implementering av ISS-rammeverk som ISO27001 og COBIT (Fazlida & Said, 2015). En kan også risikere å feile, ved at man tror alle retningslinjer er på plass og at disse blir etterlevd, noe som kan gi en falsk trygghet (von Solms & von Solms, 2004). For å imøtekomme dette problemet kan ISS-implementering bli oppnådd ved å blant annet involvere ansatte i formulering av sikkerhetsretningslinjer. På denne måten kan man unngå tilbakefall og at retningslinjene blir avvist (Fazlida & Said, 2015, s. 247). Retningslinjer for informasjonssikkerhet blir realisert ved ISS, og retningslinjer er startpunktet for et referanserammeverk hvor all informasjonssikkerhet, sub-retningslinjer, prosedyrer og standarder bør være plassert (von Solms & von Solms, 2004, s. 374). Retningslinjer kan deles inn i tre nivåer, fra det strategiske og taktiske, til det operasjonelle. Det er toppledelsen som setter de overordnede strategiske retningslinjene, som så blir brutt ned i de taktiske og operasjonelle (von Solms et al., 2011). De taktiske retningslinjene har mellomledelsen ansvar for å formidle og håndtere, slik som bruk av elektronisk utstyr og hendelsesrapportering. Det operasjonelle handler om tekniske retningslinjer for servere, internett og liknende. De ulike retningslinjene bør bli støttet opp av de overordnede retningslinjene (von Solms et al., 2011). Det er også viktig å etablere klare konsekvenser og disiplinær handling når retningslinjer ikke blir fulgt (Mishra, 2015, s. 133).

3.3.5 Sikkerhetsprogramledelse

Revisjoner og kontroll

Revisjoner og kontroll er en viktig komponent innen ISS. Her bør man identifisere virksomhetens mål og sikkerhetsmekanismer, samt identifiserer risiko som kan oppstå som følge av inadekvate prosedyrer og retningslinjer. Revisjoner bør utføres regelmessig for å hele tiden optimalisere ISS'en (AlGhamdi et al., 2020, s. 14). Det er videre viktig for en suksessfull ISS at man observerer for å holde oversikt over trusler og risiko til enhver tid (AlGhamdi et al., 2020, s. 19), og gjør regelmessige trusselvurderinger (Gashgari et al., 2017) slik at man kan håndtere nye risikoer ved endringer i prosesser og nye prosjekter. Dette gjør det mulig å aktivt respondere på nye trusler (AlGhamdi et al., 2020, s. 19). Det er også viktig at man etablere enkle og fleksible kontrollmekanismer (Mishra, 2015, s. 136).

Etterlevelse

Etterlevelse handler om at virksomheten må overholde lover og regler som gjelder for informasjonssikkerheten. En bør skape en etterlevelseskultur i virksomheten (AlGhamdi et al., 2020). Etterlevelse gjelder ikke bare internt, men også mot tredjeparter og leverandører som håndterer virksomhetens data (AlGhamdi et al., 2020, s. 12). Ansatte i en virksomhet må etterleve de lover og regler som gjelder, samt overholde standarder som ISO27001. Etterlevelse ansees som en viktig del av en strukturert tilnærming til styring (Mukundan et al., 2014, s. 7) og setter fokus på å følge regler så vel som virksomhetsretningslinjer og prosedyrer (Asnar & Massacci, 2011, s. 2).

Det å håndheve og overholde informasjonssikkerheten, i tillegg til overvåkning, er essensielt for å skape en vellykket ISS-plan (von Solms & von Solms, 2004, s. 374-375). For å kunne etterleve ISO-seriestandardene må etterlevelse av rammeverk for lover og regler følges. Å definere og lage prosesser for å identifisere hvorvidt virksomheten etterlever standardene i ISO27001 serien, er derfor viktig (Gillies, 2011). En må sørge for at oppførselen til ansatte blir overvåket og dirigert for å sikre etterlevelse av sikkerhetskrav (Veiga & Eloff, 2007, s. 363). For å oppnå dette kan man foreta målinger, utarbeide rapporter og evaluere. Å utarbeide rapporter bidrar med å beskrive tilstanden til ISS og gir en god oversikt over hvor langt man har kommet (AlGhamdi et al., 2020, s. 19).

3.3.6 Brukerfokusert sikkerhetsledelse

Informasjonssikkerhetskultur

Informasjonssikkerhetskultur er en viktig komponent i ISS og man bør skape en positiv informasjonssikkerhetskultur gjennom å oppmuntre til eksperimentering, opplæring og bevisstgjøring (Albuquerque Junior & Santos, 2015; Gashgari et al., 2017). Ved bruk av et ISS-rammeverk i en virksomhet kan det ha en positiv innvirkning på ansattes oppførsel i hvordan de sikrer virksomhetens eiendeler og opprettholder en akseptabel informasjonssikkerhetskultur (Veiga & Eloff, 2007, s. 317; Williams, 2008, s. 214).

En vellykket ISS samsvarer med at ansatte i forskjellige deler av organisasjonen har god nok bevissthet rundt informasjonssikkerheten (Wu et al., 2018). Et ISS-rammeverk kan bli brukt til å lage et evalueringsverktøy for å måle hvorvidt informasjonssikkerhetskulturen er på et

akseptabelt nivå, og igangsette planer for forbedringer (Veiga & Eloff, 2007, s. 371). Forskning viser at en etterlevelsekultur i noen tilfeller har fokusert for mye på det operasjonelle og ikke det strategiske, noe som også er viktig å ta hensyn til (Maynard et al., 2018). Bevissthet er en essensiell del av ISS og består av å skape en kultur der sikkerhet er i fremsetet hos alle nivåer i virksomheten. Å skape bevissthet gjøres gjennom linjeledelsen slik at man garanterer at alle ansatte blir informert (AlGhamdi et al., 2020, s. 6). Kultur er viktig ettersom gruppers atferd former hvert enkelt individs oppfatning av sikkerhet (Mishra, 2015, s. 132).

4. Teoretisk linse – institusjonell logikk og institusjonelt arbeid

Teorier er lite brukt i informasjonssikkerhetsforskning og det er et behov for å låne teorier fra andre felt for å oppnå en bedre forståelse (Ada et al., 2009, s. 289). De fleste ISS-rammeverkene og modellene mangler teoretisk og empirisk validering, er generiske og universelle og tar ikke hensyn til viktigheten av sosial- og atferdsfaktorer (Schinagl, 2020, s. 263). Forskningen innenfor dette feltet har hatt et for stort fokus på det praktiske aspektet og det er mangel på forskning som bruker teori som gir dypere forklaringer (Lidster & Rahman, 2018; Schinagl, 2020). Dette kapittelet redegjør for valg av teori som benyttes i studien. Teorien vi har valgt er institusjonell logikk og institusjonelt arbeid som har utspring i institusjonell teori (Thornton & Ocasio, 2008, s. 99-100) og er et forsøk på å imøtekomme behovene litteraturen peker på.

Institusjonell logikk kan være med på å forklare motstridene praksiser og oppfatninger som er iboende i institusjoner (Wahid & Sein, 2013; Williams et al., 2013) og forklare kompleksiteten rundt ISS (Williams et al., 2013, s. 352). Ettersom vi ikke kun er ute etter å identifisere utfordringer i kommuner, men også forklare årsakene til disse, fungerer denne teorien godt til dette formålet. Institusjonell logikk blir i studien brukt som en linse for å forstå og analysere ISS på en mer systematisk og dypere måte. Videre vil vi bruke institusjonelt arbeid som er et felt innenfor institusjonell teori, som ser på hvordan mennesker eller grupper bidrar til å endre, skape eller ivareta institusjoner (Lawrence et al., 2013). Dette er relevant da vi kan identifisere ulike typer institusjonelt arbeid som er nødvendig eller essensielt for å støtte ISS. Institusjonelt arbeid kan kombineres med institusjonell logikk og kan være en viktig kilde til endring i logikkene (Gawer & Phillips, 2013, s. 1060).

Bruken av institusjonell teori i forskning kan medføre noen begrensninger og utfordringer som må adresseres. Studier som bruker institusjonell teori, har ofte begrensninger ved at de kun fokuserer på det organisatoriske perspektivet og ikke ser individnivået. Det er derfor behov for at studier innen denne teorien ser på effekten av institusjonalisering og ikke kun prosess og utfall (Currie, 2009, s. 63). Forskning som bruker denne teorien bør kombinerer en eller flere teorier, gjerne fra tilsvarende felt. I tillegg bør man ta for seg det menneskelige aspektet og hvordan disse former og blir formet av institusjonene (Currie, 2009, s. 75-76). Vi har forsøkt å imøtekomme begrensningene beskrevet av Currie (2009) ved å fokusere på individer i form av informanter fra kommuner som aktivt jobber med ISS, og deres synspunkt på arbeidet og utfordringer de møter. Vi har også inkludert teorien institusjonelt arbeid, hvilket ser på hvordan individer former logikker og institusjoner som bidrar med en kombinasjon av teorier. Enkelte forskere påpeker at institusjonell logikk og institusjonelt arbeid har blitt et utydelig konsept med uklare grenser (Alvesson & Spicer, 2019, s. 205). På en annen side vil slike uklarheter være nyttig i studier som er utforskende og på utkikk etter nye ideer og konsepter (Alvesson et al., 2019, s. 112). Vi ønsker ikke å gå videre inn i diskusjonen om begrensninger og de delte meningene i faglitteraturen angående teorien, det er derimot viktig at vi erkjenner at det finnes ulike meninger.

4.1 Institusjonell logikk

Institusjoner står sentralt i forskning som bruker institusjonell teori. Det eksiterer mange definisjoner på en institusjon. En institusjon betegnes av Ronald L. Jepperson som “a social order or pattern that has attained a certain state or property” (DiMaggio & Powell, 1991, s. 145). Institusjoner kan videre betegnes som en sosial struktur hvor praksiser innenfor strukturen og rammene til institusjonen blir gjentatt av de som er involvert i institusjonen. De involverte har derfor fått en delt felles forståelse av realiteten (Kandathil et al., 2011, s. 2).

Ettersom institusjonell logikk definerer mening og innhold delt av sosiale aktører i institusjoner, er institusjonell logikk en viktig faktor for å avgrense og oppnå forståelse av et organisatorisk felt (Busch, 2019, s. 26).

Institusjonell logikk er en "gren" av institusjonell teori (Thornton & Ocasio, 2008, s. 99-100). For å forstå hva som ligger til grunn for institusjonell logikk begynner vi med å forklare institusjonell teori. Forskning som bruker institusjonell teori har tidligere studert hvordan individer eller organisasjoner blir mer og mer like som følge av press fra institusjonelle krefter, også kalt isomorfisme (DiMaggio & Powell, 1983). DiMaggio & Powell (1983) viste til tre ulike krefter som bidro til isomorfisme: "tvungne", "mimetiske" og "normative" (s.150). Scott (2001) integrerte dette arbeidet i sin forskning på institusjonell teori og kom frem til tre ulike pilarer, regulative, normative og kulturell-kognitive. De regulative handler om at virksomheter og individer blir påvirket av lover og regler. De normative handler om verdier og forventninger som befinner seg i miljøet virksomheten eller individet operer i, og den kulturell-kognitive handler om at individer har ulike identiteter (Scott, 2001, s. 77-81). Dette er alle krefter som er med på å skape isomorfisme. Selv om institusjonell logikk har likheter til både Scott (2001) og DiMaggio & Powell (1983), slik som hvordan kulturelle regler og kognitive strukturer former virksomheters strukturer, er ikke fokuset lenger på isomorfisme, men på forskjellige logikkers innvirkning på individer og organisasjoner (Thornton & Ocasio, 2008). Institusjonell logikk er således en alternativ tilnærming innen institusjonell teori som skiller seg fra DiMaggio & Powells (1983) teori om isomorfisme, samt Scott (2001) og de institusjonelle pilarene (Thornton et al., 2012, s. 47). Innen forskning på IS anbefales det å se forbi eldre institusjonell teori og rette synet mot ny-institusjonelle teorier slik som institusjonell logikk (Currie, 2009, s. 66-67).

Som nevnt i avsnittet over har institusjonell logikk sitt utspring i institusjonell teori og ble laget som en reaksjon på de teoretiske begrensningene til institusjonell teori og blir betegnet som "a metatheory of institutions that includes organizations and explains not simply homogenity, but also heterogenity" (Thornton et al., 2012, s. 15). Teorien oppstod på 1990-tallet med pionerne Friedland & Alford (1991). De skrev at de viktigste institusjonene i vestlige samfunn har en sentral logikk som har sine organisatoriske prinsipper som er tilgjengelige for virksomheter og individer å utdype (Friedland & Alford, 1991, s. 248). Eksempler på disse er blant annet demokrati, familie, religion, staten og vitenskap. Logikken er symbolsk grunnfestet, organisatorisk strukturert, politisk forsvart, samt teknisk og materialistisk begrenset, derav har de spesifikke historiske begrensninger (Friedland & Alford, 1991, s. 248-249). Thornton, Ocasio og Lounsbury (2012) definerer institusjonell logikk som "... socially constructed, historical patterns of cultural symbols and material practices, assumptions, values and beliefs by which individuals produce and reproduce their material subsistence, organize time and space, and provide meaning to their daily activity" (Thornton et al., 2012, s. 51). Institusjonell logikk sammenstiller materielle og symbolske elementer som integrerer forskning på kultur og kognisjon, og bidrar med en strategisk teori for hvordan kultur former handlinger (Thornton et al., 2012, s. 11). Med materielle elementer menes strukturer og praksiser, med symbolske elementer referer man til tankegang og mening (Thornton et al., 2012, s. 10).

Innen institusjonell logikk finnes det ulike idealtyper som er nyttig i analysearbeidet. Idealtyper er verktøy for å forstå kulturelle meninger og logiske komponenter (Thornton et al., 2012, s. 52-53). Dette hindrer forskeren fra å kun reprodusere empiri som i mange situasjoner kan virke forvirrende og forenkler analysearbeidet. Idealtypene består av hva som er essensielt rundt et fenomen og definerer begrensninger rundt institusjonelle ordener som er systematisk definert og identifisert (Thornton et al., 2012, s. 52-53). Idealtyper er en metode

for fortolkende analyse og når man lager idealtyper må det gis en beskrivelse av idealtypene og skrives ned påstander som relaterer idealtypen til den avhengige variabelen (Thornton & Ocasio, 2008, s. 110). Idealtyper beskriver hva som skjer innen et organisatorisk felt og bidrar med en analytisk modell som gjør det mulig å sammenlikne observasjoner på tvers av institusjoner (Thornton & Ocasio, 2008, s. 119). Idealtyper som ofte blir beskrevet i litteraturen, er familie, religion, stat, marked, profesjon og virksomhet. Disse typene består av ulike byggeklosser som representerer kulturelle symboler og materielle praksiser (Thornton et al., 2012, s. 54-56). Idealtypene er med på å gjøre analysen enklere og mer håndgripelig (Thornton et al., 2012, s. 52). Det er videre et verktøy for å tolke kulturelle betydninger til dens logiske komponenter og gjør det enklere å analysere dataene som gir en rik og generaliserbar forståelse av varierende prosesser (Thornton et al., 2012, s. 52). Idealtyper er ofte basert på tidligere litteratur og empiri, hvor man knytter ulike karakteristika til en idealtype-logikk (Reay & Jones, 2016, s. 446-449).

Det har vært en økende bruk av institusjonell logikk som følge av en trend der institusjonell teori blir brukt til komplekse studier (Berg Johansen & Waldorff, 2015, s. 3). Institusjonell logikk er en av flere grener av ny-institusjonell teori (Alvesson & Spicer, 2019) og har blitt brukt i økende grad på forskning innen informasjonssystemer (Busch, 2018, s. 1). Teorien er blant annet tidligere blitt brukt til å undersøke implementering og adopsjon av ERP-systemer (Berente & Yoo, 2012), IT-styring (Currie & Guah, 2007) og virksomhetsarkitektur (Dang, 2021). Institusjonell logikk har en innvirkning på oppførselen og praksiser blant ansatte i en virksomhet og det kan eksistere flere og ofte motstridende logikker i samme virksomhet (Wahid & Sein, 2013). I forskning er institusjonell logikk brukt til å blant annet måle effekten av innhold, mening og endringer (Thornton & Ocasio, 2008, s. 109). Måten dette gjøres på er gjerne gjennom historieanalyse, fortolkende metoder eller triangulering der idealtyper og data blir analysert i flere nivåer, fra individ til organisasjon og miljø (Thornton & Ocasio, 2008, s. 109).

Logikker kan blant annet overføres via reguleringsorganer, industristandarder, samt gjennom skrevne regler og forskrifter. Individer kommuniserer igjen logikkene gjennom hverdagsprat eller via skrevne tekster. Logikker begrenser hvilke handlinger som blir tatt og hvilke handlinger som er tilgjengelig (Lammers & Garcia, 2017, s. 202). Innen eierstyring og selskapsledelse hvor ISS ofte er en innlemmet del, vil en institusjonell tilnærming sette fokus på konflikter og ulikheter, se innføring av praksiser fra en institusjonell kontekst til en annen og fokusere på integrasjon og handling (Fiss, 2008, s. 401). Det vil derfor sette spørsmål ved det sammenhengende synet til nasjonale systemer for eierstyring og selskapsledelse. Slike systemer kjennetegnes av spenninger mellom forskjellige styringsmodeller og institusjonell logikk, en prosess som vil lede til endring. Endringer betyr ikke alltid større konvergens i et styringssystem, men økt variasjon mellom systemene (Fiss, 2008, s. 401). Institusjonell logikk vil videre ikke håndtere diffuse ISS-praksiser slik som ISS-rammeverk som en homogen enhet. Det vil si at institusjonell logikk presenterer forskjellige fortolkende rammer for aktører som er med på å forme ISS. ISS-praksiser former logikkene og ved å bruke dette synet kan man identifisere variasjoner i praksis (Williams et al., 2013, s. 344).

Søk i databaser viser at det finnes minimalt med forskning som tar for seg institusjonell logikk og ISS. To av artiklene vi ønsket å inkludere var Williams, Hardy og Holgate (2012/2013), som kom frem til at ISS i virksomheter blir formet av ulike lover, regler, materielle praksiser og strategiske imperativer. Dette tilsier at ulike kulturelle verdier, normer og logikker har en innvirkning på ISS og derfor trengs det forskning som knytter aktivitetene til menneskene i organisasjoner som er informert av, og tilknyttet de ulike logikkene (Holgate et al., 2012). Selv om normative institusjoner av ISS, som ISO-rammeverk, har evne til å

endre strukturer på tvers av kontekster, kan disse også endres over tid basert på oppfatninger tilknyttet ISS i lokale kontekster. Institusjonell logikk er med på å endre disse oppfatningene (Williams et al., 2013).

4.2 Logikker i offentlig sektor

I dette avsnittet forklarer vi logikker i offentlige sektor. Dette er relevant for vår studie da vi ser på ISS i norske kommuner og om det eksisterer ulike logikker innad i kommunene. I tillegg har vi identifisert ulike idealtyper for logikkene som vil gjøre analysearbeidet enklere som ble diskutert i delkapittel 4.1.

Studier som tar i bruk institusjonell logikk, tar ofte for seg hvordan menneskelig atferd blir påvirket av ulike logikker. Det handler om å identifisere hvordan ulike personer handler på bakgrunn av dominante logikker innen et felt. Virksomheter som er institusjonelt komplekse og huser mange ulike og ofte motstridende logikker kan være en kilde til frustrasjon blant de ansatte (Busch, 2018, s. 7). I det daglige arbeidet vil ansatte i kommunene møte ulike situasjoner og handlinger, og disse blir formet av ulike logikker (Fred, 2020, s. 8). To institusjonelle regimer som står sentralt i offentlig sektor er stat og marked, hvor hver av disse er karakterisert av en bestemt logikk. Generelt ses virksomhetslogikk i sammenheng med marked og administrativ byråkratilogikk i sammenheng med stat (Meyer et al., 2014, s. 863). Ved å identifisere disse på forhånd er det mulig å systematisere funn senere, noe som kan være med på å gjøre analysearbeidet enklere (Thornton et al., 2012, s. 52-53).

Innenfor offentlig forvaltning har det skjedd flere skifter i Europa der man har beveget seg noe vekk fra byråkratilogikken, og mer over til markedslogikk som går under betegnelsen "new public management" (NPM) (Meyer et al., 2014, s. 865). NPM har vært med på å forme og utfordre den etablerte kulturen i offentlig sektor i Norge, fra å tidligere fokusere på administrasjon og tjene offentlige interesser, til markedslignende organisasjons- og styringsprinsipper. Dette har ført til fokus på modernisering og effektivisering av institusjoner, i tillegg til å redusere offentlig sektors makt. Denne logikken eksisterer i Norge på statlig, regionalt og lokalt nivå (Busch & Ramstad, 2004, s. 1), og eksempelvis organisering av kommunene bygger på NPM (Hansen, 2018, para.11). Landene i Norden er noen av de som har kommet lengst i å tilpasse seg logikkene til NPM (Fred, 2020, s. 6), og selv om det har skjedd noen endringer, finnes det fortsatt byråkratilogikk i offentlig sektor i Norge (Thorbjørnsrud et al., 2014; Trondal, 2011). Byråkratilogikk har sentrale verdier som å overholde lover, stabilitet, objektivitet, sikkerhet, lojalitet og korrekthet. Det er fokus på input, ansvarsområder, plikter og rettigheter, samt de rette handlingene. Legitimiteten stammer fra prosedyre, og staten er den styrende enheten i samfunnet. Styringsmodellen er byråkratisk, basert på lover og kontroll, og har fokus på hierarkiske og sentraliserte systemer (Meyer et al., 2014, s. 865-866). NPM/markedslogikken har fokus på økonomiske, rasjonelle og resultatbaserte handlinger. Målet er å betjene innbyggerne og oppnå ulike mål. Sentrale verdier som ytelse, effektivitet, endring, fleksibilitet og innovasjon er viktig. Organisatoriske og individuelle mål, samt resultater og fokus på konsekvensen av handlinger tas hensyn til. Styringsmodellen er i hovedsak kontraktbasert, basert på mål og resultater, ytelsesmåling og ledelsesverktøy i et konkurransepreget miljø. Det bygger opp under sterk ledelsesautonomi og et desentralisert system (Meyer et al., 2014, s. 865-866).

Både kommunene og deres virksomheter vil bestå av personer med ulike profesjoner og faglige bakgrunner. Vi ønsker derfor også å inkludere profesjonslogikk, hvilket bygger på profesjonelle nettverk, personlig ekspertise, status i profesjon, samt en profesjonell assosiasjon til arbeidet (Thornton et al., 2012, s. 56). Arbeidet med, og praktisering av ISS,

kan bestå av IKT-leder, systemeier, sikkerhetsansvarlig, personvernombud og kommunedirektør (Sandefjord kommune, u.å), og representerer således personer med ulik bakgrunn og logikk. Vi tar utgangspunkt i at vi kan identifisere profesjonslogikk, markedslogikk og byråkratisk logikk i kommunene (Tabell 7). Utover logikkene vi har identifisert på forhånd er vi også åpne for å analysere og finne egne logikker da det å kun basere seg på etablerte logikker og idealtyper kan hindre ny innsikt (Reay & Jones, 2016, s. 443). Tabell 7 viser oversikt over logikker vi forventer å identifisere blant våre informanter i studien.

Tabell 7: Oversikt over logikker, basert på (Berg et al., 2017; Meyer et al., 2014).

Karakteristika /logikk	**Byråkratilogikk**	**NPM/markedslogikk**	**Profesjonslogikk**
Rasjonalitet	Byråkratisk, legalistisk, profesjonell.	Økonomisk, rasjonelle handlinger, resultatbasert.	Profesjonell
Legitimitet	Prosedyre.	Offentlig sektor som tjenesteleverandør.	Personlig ekspertise
Mål	Staten som styrende posisjon i samfunnet.	Oppnå mål, betjene klienter, kunder.	Profesjonell status
Sentrale verdier	Lovmessig, korrekt, politisk nøytral, objektiv, lojalitet, sikkerhet, hemmelighold, kontinuitet og stabilitet.	Ytelse, effektivitet, klokskap, endring, fleksibilitet og innovasjon.	Kunnskap og opplæring, tillit, profesjonelt arbeid,
Fokusområde	Regler, input, ansvarsområder, plikter og rettigheter. Fokus på de rette handlingene.	Organisatoriske og individuelle mål, resultater og fokus på konsekvensene av handlinger.	Fokus på profesjon, profesjonell interesse, arbeid, sikre at interessen av den profesjonelle gruppen samsvarer med deres prioriteter, identitet og verdier.
Styringsmodell	Byråkratisk basert på lover, fokus på direktiver og kontroll. Hierarkisk og sentraliserte systemer.	Kontraktbasert, basert på mål, resultater, ytelsesmåling, ledelsesverktøy i et konkurransepreget landskap. Desentralisert system, sterk ledelsesautonomi.	Konsensusorientert, tillit, autonomi

I tillegg til administrasjonen vil personer i kommunens virksomheter, slik som helse- og sosial, teknisk, og oppvekst, bestå av mennesker med ulik faglig bakgrunn og profesjoner, hvilket representerer ulike logikker. Hos virksomheter som skole og oppvekst finner man blant annet profesjon, marked og byråkratilogikk (Gullberg & Svensson, 2020). I helse- og

sosial ser man ofte at profesjon (Berg & Pinheiro, 2016), marked og ledelseslogikk (Berg & Pinheiro, 2016; Kristiansen et al., 2015) står sterkt og arbeiderne innen dette feltet kan ses på som politiske aktører og leddet mellom staten og befolkningen. Via deres egeninteresser kan det derfor oppstå politiske gnisninger (Berg & Pinheiro, 2016). Selv om noen logikker kan dominere er de ikke homogene på tvers av felter og kan variere i forhold til ulike sosiale settinger. En lege kan ta i bruk profesjonell logikk når h*n operer, og markedslogikk i samtaler med IT eller selgere (Thornton et al., 2012, s. 99). Dette kan derfor forklare hvorfor man ofte finner hybride logikker og man kan identifisere kombinasjoner av ulike logikker som for eksempel at sykehus kan bestå av en blanding av profesjon- og markedslogikk (Berg & Pinheiro, 2016). I neste avsnitt presenterer vi hvordan det kan eksistere ulike logikker og hva dette kan medføre.

4.3 Institusjonell pluralisme, konkurrerende logikker og samarbeidende logikker

Ettersom kommuner består av mange ulike virksomheter og personer med ulik faglig bakgrunn vil ulike logikker møtes. Når det eksisterer flere ulike logikker sammen, har litteraturen siktet til pluralisme, konkurrerende-, og samarbeidende logikker.

Forskning har erkjent den økende forekomsten av flere logikker i organisasjoner (Reay & Hinings, 2009). Dette fenomenet kalles institusjonell pluralisme, og skjer når organisasjoner er steder der flere logikker er aktive og ingen enkelt trossystem kan opprettholde dets dominans (Ajer et al., 2021, s. 5). Dette vil si at innenfor en organisasjon kan flere logikker være aktive samtidig, og selv om de to logikkene kan være gjensidig tilretteleggende, så vil det være en spenning mellom disse. Et eksempel er innen helsevesenet, hvor det ofte oppstår spenninger mellom medisinsk profesjonalitet og ledelse (Ajer et al., 2021; Reay & Hinings, 2009). Studier av organisasjoner som inneholder flere logikker antyder at det er ulike resultater på hvordan disse logikkene oppfører seg (Besharov & Smith, 2014, s. 16-17). I noen tilfeller kan logikkene være konkurrerende og skape motsetninger og endringer (Lounsbury, 2007, s. 302), i andre tilfeller kan flere logikker eksistere relativt fredelig i en organisasjon (Besharov & Smith, 2014, s. 16-17). Noen mener at tilstedeværelsen av flere logikker kan true organisasjonens ytelse (Battilana & Dorado, 2010; Besharov & Smith, 2014, s. 16-17), mens andre mener at flere logikker innad i en institusjon kan bidra til en mer innovativ, varig og bærekraftig organisasjon (Besharov & Smith, 2014, s. 16-17; Sgourev, 2011).

Flere studier har sett på hvordan logikker konkurrerer mot hverandre, men istedenfor å fokusere på konkurranse som en mekanisme for å forstå institusjonell endring, har noen teoretikere pekt på samarbeid som en viktig komponent i institusjonalisering (Reay & Hinings, 2009, s. 632). Ettersom samarbeid er en effektiv måte for aktører å handle på, er institusjonelle felt formet av samarbeidsaktiviteter gjennom utvikling av nettverk, dominanskulturer og produksjon eller vedlikehold av institusjonelle regler. Noen typer samarbeid samler ulike aktører som har forskjellig interesser, og gjennom prosessen med å håndtere interessene kan samarbeidsaktiviteter påvirke endringer i institusjonell logikk (Reay & Hinings, 2009, s. 633). Studier antyder at samarbeidspartnere har forskjellig identiteter, og for å oppnå effektivt samarbeid krever det at samarbeidspartnere delvis etterlater sin gamle identitet, og utvikler en ny identitet knyttet til samarbeidet (Reay & Hinings, 2009, s. 633). Det blir derfor oppfordret at institusjonell endring kan forekomme når aktører utvikler mekanismer for samarbeid som støtter sameksistensen av konkurrerende logikker (Reay & Hinings, 2009, s. 647).

I dette delkapittelet har vi sett at flere logikker kan eksistere sammen i en organisasjon. Logikkene kan være konkurrerende eller samarbeidende, og føre til å true organisasjoners ytelse eller bidra til en mer innovativ organisasjon. I neste avsnitt vil vi ta for oss institusjonelt arbeid ettersom dette kan være med på å påvirke og forme hvordan aktører arbeider med ISS og kan skape endringer i logikkene.

4.4 Institusjonelt arbeid

Informasjonssikkerhet er noe kommuner og offentlige virksomheter sliter med å ivareta (Digitaliseringsdirektoratet, 2020, s. 3). Nye reformer og lovgivninger som GDPR og eForvaltningsforskriften §15, er med på å skape press på kommunene, og kommunene må igjen sørge for å formidle dette videre ned til de ulike virksomhetene. Vi tror at dette kan skje via ulike typer institusjonelt arbeid. Institusjonelt arbeid blir definert som "the sets of practices through which individual and collective actors create, maintain and disrupt the institutions of organizational fields" (Lawrence & Suddaby, 2006, s. 220). Med dette menes det at personer er med på å ivareta, skape eller forhindre institusjoner i virksomheter gjennom institusjonelt arbeid. Når det kommer til å skape institusjoner finnes det ulike former av institusjonelt arbeid som fremgår i Tabell 8.

Tabell 8: Ulike former for institusjonelt arbeid, basert på (Lawrence & Suddaby, 2006, s. 221) oversatt til norsk med eksempler.

Institusjonelt arbeid
Skape institusjoner
Beslutningspåvirkning: mobilisering av politisk og regulatorisk støtte gjennom direkte og bevisste teknikker basert på sosiale overfall.
Definere: konstruksjon av regelsystemer som konfererer status eller identitet, definerer et medlemskaps grenser eller skaper statushierarkier innen et felt.
Opptjening: skapelsen av regelstrukturene som konferer eiendomsrett.
Etablere identiteter: definere forholdet mellom en aktør og feltet hvor den aktøren opererer.
Endring av normative assosiasjoner: omarbeide koblingene mellom sett av praksiser samt den morale og kulturelle grunnmuren for disse praksisene.
Etablere normative nettverk: konstruksjon av interorganisatoriske koblinger hvor praksiser blir normativt sanksjonert og hvilket former de relevante sammenligningsgrupperingene med hensyn til etterlevelse, overvåkning og evaluering.
Mimikk: assosiere nye praksiser innenfor eksisterende sett av praksiser som blir tatt for gitt, samt teknologier og regler som forenkler adopsjon.
Teoretisering: utviklingen av spesifikasjoner for abstrakte kategorier og utdypning av årsak- og virkning kjeder.
Utdanning: utdanne aktører i nye ferdigheter og kunnskap nødvendig for å kunne støtte den nye institusjonen.
Ivareta institusjoner
Muliggjøre arbeid: skapelsen av regler som tilrettelegger, supplerer og støtter institusjoner, slik som opprettelse av autoriseringsagenter eller avledende ressurser.
Politiarbeid: sikre etterlevelse med håndheving, revisjoner og overvåkning.
Avskrekking: etablering av tvangsbarrierer til institusjonell endring.
Valorisere og demonisering: tildele for offentlig konsum både positive og negative eksempler som illustrerer de normative grunnlagene i en institusjon.
Mytologisering: ivareta de normative underbyggelsene i en institusjon ved å skape og opprettholde myter knyttet til dens historie.

Innbaking og rutine: aktivt innarbeide de normative grunnlagene av en institusjonene inn i deltakernes daglige rutiner og organisatoriske praksiser.
Forhindre institusjoner
Frakoble sanksjoner: arbeide gjennom statsapparatet for å koble fra belønninger og sanksjoner fra noen sett av praksiser, teknologier og regler.
Frakoble moralske grunnlag: dissosiere praksiser, regler eller teknologi fra det moralske fundamentet som er passende innenfor den spesifikke kulturelle konteksten.
Undergrave antagelser og tro: minimere den oppfattede risikoen av en innovasjon og differensiere ved å underbygge kjerneforutsetninger og tro.

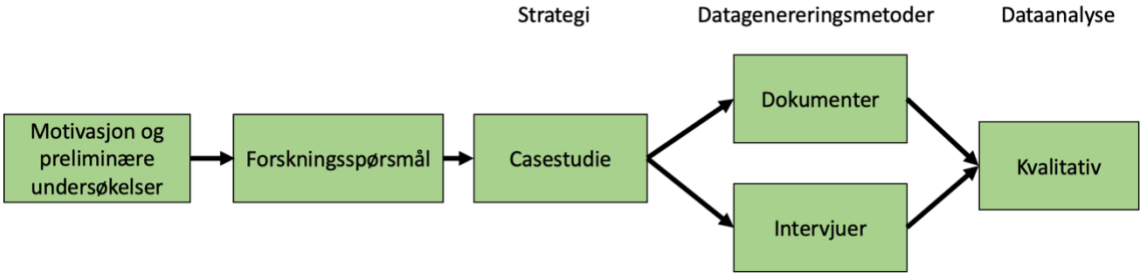
Tabell 8 viser kun eksempler på institusjonelt arbeid og er derfor ikke en fullstendig liste (Lawrence & Suddaby, 2006, s. 220). Det er viktig å nevne at institusjonelt arbeid som omhandler *forhindre institusjoner* blir betraktet som mindre vanlig og er lite adressert i litteraturen (Lawrence & Suddaby, 2006, s. 235). De ni typene arbeid som relaterer til det å skape institusjoner kan bli delt inn i tre typer: (1) "åpenlyst politisk arbeid, hvor aktører rekonstruerer regler, eiendomsrettigheter og grenser som definerer tilgang til materielle ressurser", (2) "handlinger, hvor aktørers trossystem blir rekonfigureret" og (3) "handlinger utformet for å endre abstrakt kategorisering hvor grenser og trossystemer blir endret" (Lawrence & Suddaby, 2006, s. 221). Å ivareta institusjoner består i hovedsak av å støtte og reparere eller gjenskape sosiale mekanismer som sikrer etterlevelse. Via seks ulike typer institusjonelt arbeid for å ivareta institusjoner, består de første tre av å ivareta institusjoner gjennom å sikre overholdelse av regelsystemet. De tre siste består av tiltak for å ivareta institusjoner og reproduserer eksisterende normer og trossystemer (Lawrence & Suddaby, 2006, s. 230). Institusjonelt arbeid som er med på å modifisere institusjoner, handler om å angripe og svekke de mekanismene som har ført til at medlemmene etterlever den institusjonen (Lawrence & Suddaby, 2006, s. 235). Dette kan gjøres via tre former for institusjonelt arbeid, jamfør Tabell 8.

Det er behov for mer forskning på institusjonell teori og institusjonelt arbeid i tilknytting til praktiske problemstillinger (Lawrence et al., 2013, s. 1030), og Thornton et al. (2012) anbefaler å omfavne institusjonelt arbeid og forskning rettet mot praksis (s.180). Søk i databaser som Scopus, Oria og Google Scholar (29.04.2021) viser ingen resultater på forskning som har brukt institusjonelt arbeid opp mot ISS. En kombinasjon av institusjonelt arbeid og institusjonell logikk vil bidra med et rammeverk som kan forklare institusjonelle dynamikker og bidra til dypere diskusjoner og berike vårt tankesett (Gawer & Phillips, 2013, s. 163; Zilber, 2013, s. 77). Dette kan bidra til å fremme bevissthet, ferdigheter og refleksivitet hos både individer og grupper, samt skape en forståelse av institusjoner som konstituert i mer eller mindre bevisste handlinger av individer eller grupper (Lawrence & Suddaby, 2006, s. 219). Ved å bruke institusjonelt arbeid ser man mer holistisk på institusjonelle handlinger og at aktører står ovenfor press fra mange ulike institusjoner, og ofte respondere på disse lokalt, kreativt, gradvis og mer eller mindre refleksivt. Man ønsker å se nærmere på praksis og prosesser, enn utfall, og spør "hvorfor" og "hvordan" i stedet for "hva" og "når" (Lawrence et al., 2011, s. 57). Det som knytter institusjonelt arbeid og logikker er en interesse for praksis og forståelse av handlinger. Institusjonelt arbeid og praksis er alltid formet av de tilgjengelige institusjonelle logikkene. Logikkene i kombinasjon med institusjonelt arbeid fungerer som et perspektiv som bidrar med en overordnet metateori og en teoretisk arkitektur som gjør kunnskapsbidrag mer synlig (Thornton et al., 2012, s. 179-180).

5. Metode

Å redegjøre for studiens valg av metode bidrar til å øke studiens troverdighet (Benbasat et al., 1987, s. 383), i tillegg vil et sammenhengende studiedesign øke kredibiliteten (Hyett et al., 2014). Ettersom denne studien er en kvalitativ casestudie, er det viktig å gi en beskrivelse av metoden basert på teori og bidrag i litteraturen.

Innledningsvis i dette kapittelet beskrives først det filosofiske paradigmet som er valgt i studien, deretter presenteres metoden som er benyttet. Videre presenteres og redegjøres det for utvalget som er gjort. Avslutningsvis beskrives prosessen for dataanalyse, samt en redegjørelse for etiske hensyn. Figur 5 viser en illustrasjon av forskningsprosessen.



Figur 5: Illustrasjon av forskningsprosessen basert på (Oates, s. 33)

5.1 Valg av filosofisk paradigme

Vi har valgt det fortolkende paradigmet i vår studie, da dette paradigmet ofte er assosiert med kvalitative casestudier, (Oates, s.292), vurderer spesielt konteksten til informasjonssystemer (Walsham, 1995), og dekker kontekstuelle forhold som er relevante for fenomenet som studeres (Baxter & Jack, 2008). Det fortolkende paradigme er ofte assosiert med forskjellige kulturer og omstendigheter, som fører til utvikling av forskjellige sosiale realiteter (Alharahsheh & Pius, 2020, s. 41-42). Dette passer til vår studie da vi ser på om det eksisterer ulike logikker innad i kommunene.

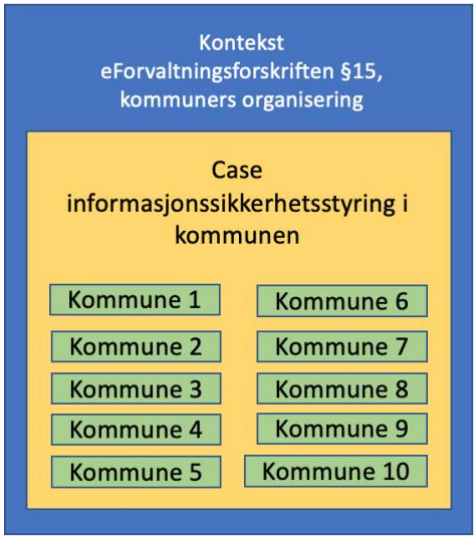
Det fortolkende paradigme blir definert som "...understanding the social context of an information system: the social process by which it is developed and constructed by people and though which it influence, and is influenced by, its social setting" (Oates, 2006, s. 292). Fortolkende studier fokuserer på menneskelige tolkninger og meninger, samt å identifisere, utforske og forklare hvordan alle faktorer i en bestemt sosial setting er relatert og gjensidig avhengig av hverandre (Oates, 2006, s. 292; Walsham, 1995). Formålet er å skape en rik forståelse av en unik kontekst, hvordan mennesker oppfatter deres verdener, og hvordan disse oppfatningene endres over tid og skiller seg fra en person eller gruppe (Oates, 2006, s. 292). I hensyn til vårt valg av teori står forskning ovenfor utfordringer med å måle effekten av innhold, mening og endring i institusjoner når de bruker institusjonell logikk. En løsning på dette vil være å ta i bruk fortolkende metoder og idealtyper (Thornton & Ocasio, 2008, s. 109). Videre vil idealtyper som diskutert i teorikapittelet, bidra med en metode for fortolkende analyse for å forstå meninger som aktører investerer i deres handlinger (Thornton & Ocasio, 2008, s. 110) og passer derfor bra til fortolkende studier. Paradigmet kan bidra med verdifulle bidrag til IS teori- og praksis (Walsham, 1995, s. 80), men det er viktig at man ikke kun fokuserer på teorien og er åpen for fortolkninger utover dette (Walsham, 1995, s. 76).

5.2 Casestudie

Studien ble utført som en kvalitativ, utforskende casestudie og omhandler ISS i et utvalg norske kommuner. En casestudie kan defineres som "...an empirical inquiry that investigates a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin, 2003, s. 13). Ettersom en casestudie bidrar til å få et rikt og detaljert innblikk i en case og dens komplekse relasjoner og prosesser, samt et detaljert bilde av hvordan relasjonene og prosessene relateres til hverandre, kan man forklare hvorfor og hvordan det gitte utfallet skjer i en bestemt situasjon (Oates, 2006, s. 141-142). Dette passer godt til vår studie ettersom vi ønsker å gå i dybden på hvordan ISS blir brukt og eventuelle utfordringer kommunene står ovenfor. Casestudier har blitt mye brukt i IS-disiplinen (Oates, 2006, s. 149) og bidrar med en allsidig strategi for IS-forskning som gjør det mulig å undersøke et fenomen i dens naturlige setting, lære av nåtidens løsninger og praksiser, få en dypere forståelse rundt komplekse fenomener og fungerer bra i forskning på underrepresenterte områder innen IS (Irani et al., 1999, s. 196-197). Casestudier kjennetegnes ved at caset studeres i en kontekst, er bundet av tid, rom og aktivitet, er inngående, bruker flere kilder som forklaring (intervju, dokumenter osv.) og varierer i ulike design (Harrison et al., 2017).

I denne studien brukes et enkeltcasestudiedesign. Forskningsdesignet gjør det mulig å gå i dybden i caset om hvordan norske kommuner jobber med ISS fra et bredt utvalg av kommuner. Målet er ikke å sammenlikne kommuner og enkelte caser med hverandre, men å identifisere utfordringer og gode løsninger som fremmer ISS. Videre ønsker vi å få et bredt bilde av hvilke logikker som brukes i relasjon til ISS. Et slikt design gjør det mulig å analysere data opp mot caset og på tvers av informantene (Gustafsson, 2017).

Det er mange definisjoner på hva som er et case, som kan være personer, grupper, virksomheter, forhold, hendelser, prosesser, problemer eller andre spesifikke enheter (Harrison et al., 2017; Langley & Royer, 2006). Caset kan undersøkes i ulike kontekster som for eksempel steder og rom (Stake, 1995). Kontekst er viktig for å forstå caset, og kan bestå av ulike variabler som politiske, økonomiske, sosiale, kulturelle, historiske og organisatoriske faktorer (Harrison et al., 2017). I studien relaterer vi caset til ISS og fenomenet som studeres, der analyseenhetene er de enkelte kommunene (kommune 1-10). Konteksten består av norske kommuners oppbygning og eForvaltningsforskriften §15 (se Figur 6 for en oversikt over casestudiedesignet vi bruker). En full beskrivelse av case og kontekst fremgår i Kapittel 6.



Figur 6: Sammenheng mellom kontekst og case

5.3 Kvalitativ metode

Vi har valgt et kvalitativt design da styrkene til denne metoden ligger i å forstå betydningen og konteksten av studerte fenomener, spesielle hendelser og prosessene som utgjør disse fenomenene over tid, i virkeligheten og naturlige omgivelser (Kaplan & Maxwell, 2005, s. 31). Da denne studien ikke er en langtidsstudie har vi ikke undersøkt fenomenet over tid, men vi har spurt informantene om tidligere hendelser og erfaringer for å få dypere forklaringer. Kvalitativ forskning bruker data i form av ord, lyd og bilder, som samles inn ved bruk av intervjuer, observasjoner og dokumenter, og gjennomføres i en naturlig setting (Kaplan & Maxwell, 2005, s. 30; Oates, 2006, s. 266). Kvalitative metoder fungerer bra til å studere institusjonell logikk, og omtrent 66% av artiklene innenfor denne teorien bruker denne metoden (Reay & Jones, 2016, s. 441). Kvalitative metoder er også nyttig for å skaffe en forståelse om institusjonell logikk, ettersom det å undersøke meningsskaping ligger i kjernen av institusjonell logikk (Thornton et al., 2012, s. 145).

5.4 Datainnsamling – intervjuer og dokumenter

Vi har valgt å hente inn data via semistrukturerte intervjuer og dokumenter. Intervju er en av de vanligste metodene for datainnsamling, og semistrukturert format er den mest brukte intervjuteknikken (Kallio et al., 2016). I tillegg er intervjuer en av de viktigste kildene til data i en casestudie (Yin, 2014, s. 110). Vi har valgt å gjøre semistrukturerte intervjuer, der de involverte partene snakker om ulike sammenhenger til et gitt tema, det er en relativt åpen samtalemåte, samtidig som det følges et oppsett (Jacobsen, 2010, s. 56; 2015, s. 146-147; Kallio et al., 2016). Dette gjør det mulig for oss å gå i dybden av caset og fange opp nyanser og delte meninger som kan være formet av de ulike logikkene. Basert på det informanten sier, kan forskeren improvisere med oppfølgingsspørsmål, noe som kan føre til at man kan få ny innsikt som man ikke visste om på forhånd (Kallio et al., 2016). I tillegg er intervjuer målrettet, da det fokuserer direkte på casets tema (Yin, 2014, s. 106).

Videre har vi valgt å inkludere dokumenter slik som veiledere og rapporter fra offentlig forvaltning. Disse dokumentene har vært tilgjengelige på nett og blitt inkludert som en del av funnene for å vise hvordan norske kommuner jobber med ISS, utfordringer, bidra til diskusjon og vise gode eksempler. Dokumenter i kombinasjon med intervjudata kan bidra til å redusere forskningsbias ved å bekrefte funn på tvers av datasett, og øke troverdigheten til studien (Bowen, 2009, s. 28). Dokumenter i kombinasjon med intervjuer er en mye brukt datainnsamlingsmetode i forskning på institusjonell logikk (Reay & Jones, 2016). På bakgrunnen av dette mener vi at et datagrunnlag hentet fra semistrukturerte intervjuer og dokumenter passer godt til vårt formål for å få en dypere forståelse om case og kontekst. I neste delkapittel vil vi redegjøre for utvalg av informanter, samt gi en oversikt over intervjuene.

5.5 Utvalg av informanter

Ettersom man innen fortolkende forskning rapporterer ens egen fortolkning av andre menneskers fortolkninger, er det viktig å skape kredibilitet og redegjøre nøye for utvalget som er gjort (Walsham, 1995, s. 78-79). Informantenes posisjon og informasjon ligger til grunn for de valgene som er gjort når det kommer til utvalgskriterier for informantene. Ved valg av informanter er det viktig at de er kvalifisert til å gi informasjon og kunnskap (Yin, 2014, s. 95) som best passer vårt case. Informantenes posisjon i kommunen legger derfor grunnlaget for hva slags erfaringer og informasjon de har om problemstillingene for å kunne gi et innholdsrikt og bredt bilde av det som forskes på i studien. Vi har valgt å ta i bruk

målrettet utvalg som utvalgsmetode. Ved å velge enkeltpersoner og dokumenter i caset, kan målrettet utvalg fokusere i dybden på et fenomen. Det lar deg i tillegg utforske informasjonsrike caser der man kan lære mye om spørsmål av sentral betydning for forskningen (Schoch, 2016, s. 248-249). Vi tok utgangspunkt i organiseringen i styringsdokumentet til Sandefjord kommune som lå ute på nett hvor de ulike rollene involvert i ISS var beskrevet (Sandefjord kommune, u.å, s. 6-7). På bakgrunn av dette har vi inkludert mennesker i kommuner som er involvert i ISS, og for eksempel har posisjoner som informasjonssikkerhetsansvarlig, kommunedirektør, konsulenter, rådgivere og personvernombud. Det varierte utvalget representerer folk med ulike posisjoner, hvilket er med på å redusere såkalt "elite-bias" som kan oppstå om man bare baserer utvalget på toppledelse slik som direktører, styreledere osv. (Myers & Newman, 2007, s. 22).

Av totalt 356 kommuner i Norge, ble kommunene utvalgt som en kombinasjon av kjennskap til kommunene, i form av korrespondanse vi hadde i starten av arbeidet med studien, samt tilgang. I tre av kommunene fikk vi to eller tre informanter, hvorav vi i de resterende syv kommunene fikk en informant. Vi sendte ut forespørsel om deltakelse i studien til 28 kommuner og sendte ut e-post til både små og mellomstore kommuner. I denne studien definerer vi små kommuner med et innbyggertall på 0 – 24 000 (L), og mellomstore kommuner med et innbyggertall på 25 000 - 65 000 (MS). Vi brukte chatroboten "Kommune Kari" og søkte "informasjonssikkerhetsansvarlig/kommunedirektør/personvernombud", hos de kommunene som hadde dette, for å finne kontaktinformasjon. Hos kommunene som ikke hadde en chatrobot, fant vi kontaktinformasjon via hjemmesiden til kommunene. I noen av tilfellene ble vi videresendt til personer som hadde informasjon om vårt tema. Flere kommuner svarte at på grunn av den pågående pandemien hadde de ikke kapasitet til å stille til intervju, selv om de mente dette var et viktig og spennende tema. Det var flere av kommunene som ikke svarte på e-post, og vi ringte derfor seks av kommunene direkte (kommunedirektør eller personvernombud), og fikk positive tilbakemeldinger på tre av disse, som stilte opp til intervju. Vi brukte også "snøballmetoden" (Patton, 1990, s. 176) og spurte "hvem andre kan vi snakke med som har kjennskap til informasjonssikkerhetsstyring?". På denne måten ble vi i noen tilfeller satt i kontakt med andre personer innad i kommunen, og utvalget videre ble basert på personene vi fikk anbefalt av den første informanten.

Totalt ble det gjennomført 16 semistrukturerte intervjuer i 10 ulike kommuner, hvorav to av disse intervjuene var preliminære. De preliminære intervjuene ble gjort i starten av studien for å få en oversikt og diskusjon rundt relevante temaer om informasjonssikkerhet. De 14 intervjuene som utgjør hoveddataene, inkluderer informanter som i sin rolle har et forhold til ISS. Som følge av den pågående Covid-19 situasjonen, har vi gjennomført alle intervjuene digitalt. Dette har gitt oss mulighet til å snakke med kommuner over hele Norge, da vi ikke har måtte reise til de gitte kommunene, og ikke blitt begrenset til områdene i nærheten av vårt bosted. Tabellen nedenfor viser en oversikt over informantene, inkludert koder (A-L), for å sørge for deres anonymitet. Bokstavene er en betegnelse for kommunen, der tallene viser hvor mange informanter vi har i hver kommune. I tabellen har vi også med størrelsen på kommunene, der MS står for mellomstor kommune, hvorav L står for liten kommune. Intervjuene varte i 30-120 minutter, med et gjennomsnitt på 50 minutter. Neste delkapittel gir en forklaring på hvordan vi forberedte og gjennomførte intervjuene.

Tabell 9: Intervjuoversikt

Intervjuoversikt						
	Kommune-kode	Informant	Stillingstittel	Bakgrunn	Varighet	Størrelse på kommune
1	A	A1	Personvernombud	IT teknisk og på leverandørsiden 12 år, personvernombud i 10 år.	59 min	MS
2	A	A2	Fagansvarlig i informasjons-sikkerhet	Konsulent og konsulentleder i 30 år, vært i nåværende stilling i 1,5 år.	1 time og 53 min	MS
3	B	B1	Daglig leder IKT	Jobbet med IT-systemer i 15 år, hatt nåværende stilling i litt over 1 år.	30 min	MS
4	C	C1	Digitalisering og utvikling	Sosionom med videreutdannelse innen velferdsteknologi. Jobbet i 20 år i kommunen. Hatt nåværende stilling i 1 år.	42 min	MS
5	C	C2	Sikkerhets-ansvarlig	Jobbet i kommunal sektor i 30 år som økonomisjef, assisterende kommunedirektør, fungerende kommunedirektør. Vært i nåværende stilling i fem måneder.	45 min	MS
6	C	C3	Personvernombud og beredskaps-koordinator	Sykepleier med tilleggsutdanning innenfor organisasjonsteori og ledelse, men også informasjonssikkerhet	30 min	MS
7	D	D1	Rådgiver personvern og sikkerhets-ansvarlig	Vært i hæren i 15 år, Begynte i kommunen på 90tallet, hatt ulike roller som beredskap, ansvar for informasjonssikkerhet.	1 time og 10 min	MS
8	E	E1	Personvernombud	Juristbakgrunn, saksbehandler i 10 år, advokat i 8 år. Hatt nåværende stilling i 1 år.	45 min	MS
9	F	F1	Beredskaps-koordinator og personvernombud	Militærbakgrunn, litteraturviter.	37 min	L
10	G	G1	Digitaliserings-rådgiver	Ingeniør, har jobbet som utvikler og i IT-avdeling i bank. To år i nåværende stilling.	50 min	L
11	H	H1	Informasjons-sikkerhetsansvarlig	Jobbet i kommunen siden 1998, ulike roller. Master i helseinformatikk. I dag informasjonssikkerhet og digitalisering.	55 min	L

12	H	H2	Konsulent med ansvarsområder innenfor virksomhets-styring og internkontroll	Utdannelse innen økonomi, revisjon og ledelse. Jobber i dag med virksomhetsstyring og prosesser.	55 min	L
13	I	I1	Rådgiver, tjenestedesign og kvalitetsutvikling	Utdannet lærer, jobbet som lærer i 18 år, byråkrat i skoletjenesten, jobbet med å innføre teknologi i grunnskolen.	30 min	MS
14	J	J1	Kommunedirektør	26 år i forsvaret, vært kommunedirektør, fylkesmann og nå kommunedirektør.	40 min	L
Preliminære intervjuer						
15	K	K1	Digitalisering og utvikling i en kommune		50 min	MS
16	L	L1	HelseCERT		45 min	

5.6 Gjennomføring av intervjuer

Før vi intervjuet informantene utarbeidet vi en intervjuguide. Vi har basert intervjuguiden vår på problemstillingen, da målet var å få frem synspunkter om hvordan informasjonssikkerhet styres i kommunene. Det teoretiske perspektivet ble ikke brukt deduktivt til å forme intervjuguiden da vi ønsket å bruke en induktiv tilnærming hvor vi spurte generelt om arbeidet med ISS og utfordringer de hadde. Eksempler på spørsmål finnes i intervjuguiden (Vedlegg 1). En intervjuguide er nyttig å bruke under intervjuet for å komme inn på aktuelle tema og stille riktig spørsmål (Jacobsen, 2015, s. 150-151). Vi lagde først en generell intervjuguide som fikk frem spørsmål vi ønsket svar på. I tillegg leste vi oss opp på kommunene vi skulle snakke med før intervjuet for å se om det fantes informasjon om ISS på internett. I noen tilfeller justerte vi på den generelle intervjuguiden, for å stille spørsmål tilpasset til den gitte informanten. Eksempel er informanter som jobber i operasjonelle roller og som derfor ikke jobber direkte med styring slik som daglig leder IKT-samarbeid og rådgiver i tjenestedesign og kvalitetsutvikling. Før intervjuet fikk informantene tilsendt et samtykkeskjema. Dette inkluderte informasjon om studien, hva deltakelse i studien innebærer, hva som skjer med informasjonen om deltakerne, at deltakelsen er frivillig og hvor lenge intervjuet vil vare (Vedlegg 2). Alle informantene signerte samtykkeskjema før intervjuet.

Vi startet intervjuene med en introduksjon av forskingsprosjektet og informerte deltakerne om anonymitet og konfidensialitet. Vi ønsket å benytte oss av lydopptak for å transkribere de ulike intervjuene i ettertid, og for å få en fullstendig oversikt når dataene analyseres. På bakgrunn av dette spurte vi om det var greit at vi gjorde lydopptak av intervjuet og forklarte at vi brukte godkjent diktafon lånt fra UiA, at dette lagres på UiA sin server og blir slettet når studien er levert inn. Alle informantene samtykket til lydopptak. Vi presiserte også at informanten har rett til å ikke svare. Under intervjuene ble det brukt ulike teknikker, som "speiling" (Myers & Newman, 2007, s. 22), der vi gjentok noen av informantenes utsagn for å vise interesse og forståelse. Dette en teknikk som gjør at man kan redusere risikoen for å stille ledende spørsmål hvor forskeren tvinger sine verdenssyn over på informanten (Myers & Newman, 2007, s. 22). Fleksibilitet, improvisasjon og åpenhet er også viktig når man samler inn data fra semistrukturerte intervjuer (Myers & Newman, 2007, s. 17). I flere av intervjuene har dette blitt brukt når informanten har hatt begrenset kjennskap til ISS og vi har da brukt

alternative inngangsmåter for å få frem informantens syn som, "prat om hvordan dere jobber med informasjonssikkerhet" eller liknende.

Det å være nøytral, respektiv, høflig og profesjonell under intervjuet vil være viktig som forsker (Oates, 2006, s. 188-189) for å ikke påvirke informantens svar og synspunkt. Vi spurte derfor om det var greit å bruke direkte sitater fra informanten i studien. Noen informanter ønsket å lese gjennom sine sitater, og de fikk derfor disse tilsendt. Vi presiserte at det ikke var anledning til å "pynte" på sitatene, og at gjennomlesningen var for å se om vi hadde oppfattet informanten riktig. Vi tok notater under intervjuet, da dette kan være positivt for å gjøre det enklere å komme med oppfølgingsspørsmål. Det er også anbefalt at man avslutningsvis spør om noe ikke er dekket (Oates, 2006, s. 193), derfor var det viktig å sette av litt tid på slutten av intervjuet. Vi avsluttet med å takke informantene for deltakelsen og at de tok seg tid til å snakke med oss. I etterkant av intervjuene, ble materialet transkribert, noe som gjorde det enklere å analysere dataene (Oates, 2006, s. 193).

5.7 Dataanalyse

Vi har vært to personer som både har innhentet og analysert data. Dette gjør det mulig å innhente rikere data og man kan være mer selvsikker og stole mer på nøyaktigheten i dataene (Benbasat et al., 1987, s. 374). Kvalitativ dataanalyse innebærer å trekke ut lyder, verbale eller visuelle temaer og mønster som er viktig for, og passer vårt forskningstema (Oates, s.267). Etter ferdig transkriberte intervjuer, benyttet vi NVivo til å analysere og søke i dataene, samt til å lage kategorier og koder. Tabellen under Vedlegg 3 viser en oversikt over kategoriene vi brukte i NVivo.

I studien er datainnsamlingen og analysen gjort med en kombinasjon av en induktiv og en deduktiv tilnærming ved å identifisere kategorier som er observert i dataen og kategorier som forekommer når man leser datamaterialet (Oates, s.269). Kodene i NVivo er basert på konseptdrevne kategorier som er basert på teori og tidligere forskning (Schreier, 2014), hvilket forbindes med en deduktiv tilnærming (Oates, s.269). I tillegg har vi inkludert datadrevne kategorier (Schreier, 2014, s. 9) som er basert på en induktiv tilnærming (Oates, s.269), hvor vi kategoriserte basert på dataene vi fikk inn fra intervjuene. Normalt vil man kombinere disse kategorier ved å bruke de datadrevne kategoriene som subkategorier (Schreier, 2014, s. 9), men ettersom institusjonell logikk har egne karakteristika som beskriver logikken, vil subkategoriene kun bestå av konseptdrevne kategorier. For å sikre at kodene og kategoriene er gode nok bør man konsultere med en ekspert innen feltet (Schreier, 2014, s. 13). Vi tok derfor kontakt med førsteamanuensis Peter Andre Busch ved UiA som har skrevet både doktorgrad og flere artikler om institusjonell logikk, til å gjennomgå disse. Vi har også brukt de samme kategoriene og underkategoriene for dokumentanalysen som med intervjudataene, hvilket er en mye brukt tilnærming til dokumentanalyse (Bowen, 2009, s. 32). Oversikt over dokumentene vi har brukt i analysen fremgår i Tabell 10.

Tabell 10: Oversikt over dokumenter fra offentlig forvaltning

Dokumenter fra offentlig forvaltning	
Digitaliseringsdirektoratet rapport om ISS i kommuner (Digitaliseringsdirektoratet, 2020)	Digitaliseringsdirektoratet (2020)
NorSIS, rapport om kommune CERT – utredning av behov og muligheter (NorSIS, u.å)	NorSIS (u.å)
Forvaltningsrevisjon av informasjonssikkerhet, drift og sårbarhet. Sandnes kommune (Rogaland Revisjon IKS, 2019)	Revisjon Sandnes kommune (2019)

Videre brukte vi en "mønstermatching" (Reay & Jones, 2016) til å identifisere logikkene. Dette vil si at vi sammenliknet data fra intervjuene med logikkene beskrevet i teorikapittelet. I tillegg ønsket vi å være åpne om å finne andre logikker enn de som er spesifisert tidligere i studien, slik at vi ikke hindret ny innsikt til alternative logikker (Reay & Jones, 2016).

Dataene er delt inn etter ulike hovedtemaer slik som informasjonssikkerhetsstyring, institusjonell logikk og institusjonelt arbeid. Hvert tema har ulike kategorier og underkategorier. Disse kategoriene er basert på både data fra intervjuene (datadrevne kategorier) og konsepter fra teori og litteratur (konseptdrevne kategorier). Vi fant frem til de datadrevne kategoriene ved å undersøke ulike sitater og ord som gikk igjen, og som vi tolket som viktig i arbeidet med ISS. I NVivo kan man se hvor mange sitater som relaterer til hvert konsept, og for eksempel underkategorien "ressurser", ble sitert seks ganger. Eksempel på et sitat om ressurser:

> "Når det gjelder ressurser for å ivareta internkontroll og informasjonssikkerhet står det i referatet fra kommunedirektørens ledergruppe at kommunen har utfordringer med å bistå, veilede og følge opp. Sikkerhetsansvarlig sier at dette er et ressursspørsmål".

Ressurser var noe som ble omtalt av flere informanter som en utfordring, og vi valgte derfor å lage underkategorien "ressurser" under hovedkategorien "utfordringer", og hovedtemaet "informasjonssikkerhetsstyring". Ettersom vi ikke kun ønsket å se på utfordringer, men også beste praksis og fremmere av ISS, laget vi også hovedkategorien "fremmere". De to resterende hovedkategoriene, "institusjonell logikk" og "institusjonelt arbeid" har underkategorier basert deduktivt på teorien. Data ble også fordelt flere steder, en utfordring kan for eksempel være forklart som følge av en institusjonell logikk og en fremmer kan forklares av institusjonelt arbeid. Dette var med på å gi en god oversikt over koblingen mellom teorien og kategorier basert på litteraturgjennomgangen og empirien.

Når det kommer til de konseptdrevne kategoriene har disse blitt brukt under hovedtema "informasjonssikkerhetsstyring", men har blitt mest brukt under institusjonell logikk og institusjonelt arbeid. De ulike institusjonelle logikkene og underkategoriene baserer seg på Tabell 7 i teorikapittelet og bygger derfor på deduktive og konseptdrevne kategorier. Innen institusjonelt arbeid baserer underkategoriene seg på Lawrence & Suddaby's (2006) kjennetegn på ulike typer institusjonelt arbeid. Vedlegg 3 viser en oversikt over data og konseptdrevne kategorier samt hovedtemaene hentet fra NVivo.

5.8 Kvalitetskriterier

I dette delkapittelet vil vi først diskutere utfordringer relatert til intervjuer og dokumenter. Deretter beskriver vi ulike kvalitetskriterier som er brukt i studien for å imøtekomme noen av disse utfordringene og for å oppnå høyere kvalitet på studien. Det er viktig å påpeke at ingen av forfatterne av studien har et personlig kjennskap til informantene fra før.

En utfordring med intervjuer er at det kan være en risiko for å stille spørsmål som ikke relaterer til studien eller dens interesseområder (Myers & Newman, 2007). Intervjuer kan mangle relabilitet, være villedende og fokusere på hva informanten sier de gjør/tenker istedenfor hva som faktisk gjøres (Oates, 2006, s. 198). I tillegg kan intervjuer være kunstig fordi informanten vet at det blir gjort lydopptak og kan gi falske inntrykk fordi de ikke vil si feil, eller at informanten sier det de tror forskeren vil høre (Yin, 2014, s. 106). Vi erkjenner også risikoen for å stille ledende spørsmål til informantene for å få svar på det man ønsker. En kilde til kritikk mot dokumentanalyse er at det kan være vanskelig å finne informasjonen man leter etter, rapporteringsskjevhet, samt at informasjon bevisst kan holdes tilbake (Yin, 2014, s. 106). For å minimere risikoen for disse utfordringene har vi brukt kvalitetskriteriene som er beskrevet i neste avsnitt og Tabell 11.

Kvalitetskriterier som validitet og relabilitet er basert på en positivistisk forskning. Fordi det i studien brukes en fortolkende tilnærming, er det derfor andre kvalitetskriterier som ligger til grunn. Troverdighet eller nøyaktighet i en studie referer til graden av tillit til data, tolkninger og metoder som brukes for å sikre kvaliteten på en studie. I enhver studie bør forskere etablere prosedyrer som er nødvendige for at en studie skal anses å være verdifull av leserne (Connelly, 2016, s. 435). Kriterier skissert av Lincoln og Guba (1989) er akseptert av mange kvalitative forskere (Connelly, 2016, s. 435) og vi har derfor valgt å ta utgangspunkt i disse. Tabellen nedenfor beskriver kvalitetskriteriene, samt viser hvordan vi oppnår disse i vår studie.

Tabell 11: Oversikt over kvalitetskriterier, basert på (Guba & Lincoln, 1989, s. 233-243; Oates, 2006, s. 294-295)

Kvalitetskriterier	Beskrivelse	Hvordan oppnå kvalitetskriterier i studien
Bekreftbarhet	Sikre at data, tolkninger og resultater er forankret i sammenhengen og ikke bare et resultat av forskerens forestillinger.	For å oppnå *bekreftbarhet* har vi forsøkt å gjøre så mye data tilgjengelig som mulig. Dette har blitt begrenset til en viss grad, ettersom vi måtte balansere hvor mye data som presenteres og samtidig opprettholde konfidensialitet hos informantene. Prosessen med hvordan vi har transformert rådata til resultater er beskrevet og vi har etter beste evne prøvd å basere resultatene på konteksten av studien.
Pålitelighet	Hvor godt forskningsprosessen er dokumentert, slik at leseren kan følge prosessen og forskerens valg.	For å oppnå *pålitelighet* har vi forsøkt å gi en god beskrivelse av metodevalgene som er tatt i studien, og grunnlaget for hvorfor disse valgene er tatt. Dette gjøres gjennom forskningsmetoden og skal gi andre forskere og leseren informasjon om hvordan denne forskningen ble utført slik at de kan oppnå samme metodiske tilnærming.
Troverdighet	Å etablere samsvar mellom de konstruerte realitetene til informantene og de realitetene som representert av forskeren. Om forskningsfunnene er	For å oppnå *troverdighet* har vi prøvd å være nøytrale og presentere funnene på en direkte måte. I tillegg presenterte vi informantenes uttalelser og konteksten de ville bli brukt i, for informantene, for å gi dem mulighet til å kommentere eller forklare betydningen bak

	beskrevet nøyaktig slik at de er troverdige.	uttalelsen for å sikre at vår tolkning var riktig. Dette er viktig for å sikre at årsaksforhold gjenspeiler hvordan fenomenet som studeres virkelig er (Guba & Lincoln, 1989, s. 236-241). Speiling ble også brukt for å vise interesse og forståelse ovenfor informanten (Myers & Newman, 2007, s. 22).
Overførbarhet	Presentere en tilstrekkelig detaljert redegjørelse for funnene for at leseren skal kunne bedømme hvordan de kan overføres til andre sammenhenger.	For å oppnå *overførbarhet* har vi forsøkt å presentere funnene på en detaljert måte slik at andre forskere kan bedømme funnene og avgjøre om, og hvordan de kan overføres til andre sammenhenger. I tillegg har vi gitt en rik beskrivelse av kontekst og fenomen (Kapittel 6) som gjør det mulig for andre å vurdere funnenes overførbarhet (Carcary, 2009)

5.9 Forskningsetiske retningslinjer

I studien har vi tatt utgangspunkt i UiAs fire grunnverdier, åpenhet, tillit, ansvar og respekt, for forskningsetikk (UiA, u.å), samt NSD sine retningslinjer. Vi sendte ut samtykkeskjema til de vi intervjuet, slik at de var innforstått med studiens omfang, og signerte før vi startet intervjuet. Konfidensialitet er viktig når man samler inn data (Oates, 2006, s. 59) og vi sikret at vi anonymiserte datamaterialet, slik at informantene ikke kan gjenkjennes direkte eller indirekte. I tillegg sikret vi at dataen vi har samlet inn ikke ble stjålet, og lagret dette på UiA sin server. All dokumentasjon i studien er lagret via Microsoft Teams knyttet opp mot Sharepoint som er tilgjengelig for studenter ved UiA, gjennom UiA sitt intranett.

Basert på Yin (2014) gir lydopptak av intervjuer en mer nøyaktig gjengivelse enn ved å ta egne notater (s.110). Imidlertid, skal det ikke gjøres lydopptak hvis a) informanten nekter tillatelse eller er ukomfortabel i dens nærvær, b) hvis det ikke er en spesifikk plan for transkribering, c) forskeren er uerfaren med tekniske enheter slik at opptaksprosedyren skaper distraksjoner under et intervju, eller d) at forskeren mener at lydopptakeren er en erstatning til å lytte nøye gjennom hele intervjuet (Yin, 2014, s. 110). Det var derfor viktig for oss å spørre informantene om det var greit å gjøre lydopptak før vi startet intervjuet. Vi brukte UiA sin håndholdte diktafon som er kompatibel med å overholde konfidensialitet. For å beskytte informantenes rettighet til anonymitet, har vi valgt å fjerne deler av noen uttalelser, hvis uttalelsen inneholdt noe som gjorde det mulig å identifisere personen eller kommunen. For å anonymisere kommunene har vi valgt å ikke definere størrelsen i innbyggertall, kun om det er en liten eller mellomstor kommune. Kommunene er heller ikke navngitt. Informantene i denne studien har vekslet med å bruke ordet "rådmann" og "kommunedirektør". Dette er to titler som har samme betydning, og for å forenkle lesbarheten i studien har vi derfor valgt å kun bruke kommunedirektør, og har i noen sitater endret fra rådmann til kommunedirektør. Videre har vi etterstrebet å ikke endre meninger eller intensjoner på uttalelser fra informantene.

Før vi startet med studien, krevdes det noen forberedelser for å kunne samle inn data og gjennomføre studien. Norsk senter for forskningsdata (NSD) er et nasjonalt senter og arkiv for forskningsdata som gjør det mulig å samle inn data om mennesker og samfunn i sammenheng med forskning. NSD bidrar til å håndtere og arkivere data med lovlig grunnlag for å sikre og ivareta personvern (NSD, u.å-b). "Personopplysninger er enhver opplysning

som kan knyttes til en person" (NSD, u.å-a). For å få lov til å samle inn personopplysninger om informantene vi ønsket informasjon fra, måtte et meldeskjema utfylles. Vi startet prosessen med NSD før jul (10.12.2020) for å sikre godkjennelse før datainnsamlingen og fikk raskt godkjent meldeskjema (14.12.2020). Ved første innsending av meldeskjema hadde vi ikke landet en konkret problemstilling, og da vi i januar begynte å lese oss nøyere opp på teori, samt hadde korrespondanse med ulike aktører, landet vi etter hvert på et endelig tema og problemstilling. Det var derfor nødvendig å oppdatere meldeskjemaet vårt til NSD, og vi endret på både problemstillingen og la ved ny intervjuguide. Vi registrerte nye endringer (19.01.2021, Vedlegg 4), og fikk godkjent meldeskjema (26.01.2021). På bakgrunn av godkjent meldeskjema kunne vi fra denne datoen samle inn empiri i form av intervjuer. I neste kapittel gis en oversikt over caset og forskningsskonteksten i studien.

6. Forskningskontekst og casebeskrivelse

Formålet med dette kapittelet er å gi en oversikt over konteksten og caset i studien, slik at leseren forstår kompleksiteten rundt det som studeres og kan beslutte om studien kan overføres til sin egen situasjon (Baxter & Jack, 2008, s. 555; Fàbregues & Fetters, 2019). Konteksten relaterer til hvordan kommuner er styrt og hvilke regler og lover som påvirker ISS. Videre handler caset om arbeidet med ISS i kommuner. En slik beskrivelse kan være nyttig for andre forskere som ønsker å gjennomføre en lignende studie under tilnærmet like forhold eller omgivelser.

6.1 Forskningskontekst

Etter sammenslåingen av flere kommuner i 2020, har vi i dag 356 kommuner i Norge (Regjeringen, u.å). Sammenslåingen skal gi større og sterkere kommuner som kan levere bedre tjenester og bedre lokalsamfunnet for innbyggere (Regjeringen, u.å). Kommunene er delt opp i ulike virksomheter hvor det drives aktiviteter som faller innenfor en bestemt næringsgruppe (Statistisk sentralbyrå, 2016, s. 4). Kommunenes virksomheter består blant annet av administrasjon, undervisning/oppvekst, helse og omsorg, kultur, teknisk drift og næringsvirksomhet (Statistisk sentralbyrå, 2016). Selv om kommuner og fylkeskommuner er selvstendige, folkevalgte og selvstyrte organer, skal styringen skje i samsvar med prinsippene for statlig styring. Disse prinsippene er lagt til grunn av skiftende regjeringer og Storting (Kommunal- og moderniseringsdepartementet, s. 10). I Norge er det de politisk valgte organene som har avgjørelsesmyndighet om hvordan det administrative apparatet i kommuner og fylkeskommuner skal organiseres, også når det gjelder organisering av arbeidet med informasjonssikkerhet (Digdir, 2020, s. 7).

Det er ulike regelverkskrav som gjelder for et styringssystem for informasjonssikkerhet. Kravene spesifiserer at offentlige virksomheter bør ha egeninteresse i et systematisk arbeid med informasjonssikkerhet (Digitaliseringsdirektoratet, u.å). eForvaltningsforskriften § 15 stiller krav til styring og kontroll med informasjonssikkerhet ved all informasjonsbehandling som offentlige virksomheter har ansvar for (Digitaliseringsdirektoratet, u.å). I henhold til forskriften skal virksomhetens sikkerhetsmål og strategi danne grunnlaget for forvaltningsorganets styring og kontroll på informasjonssikkerhetsområdet. Arbeidet med ISS skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks. ISS bør basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet og være en integrert del av virksomhetens helhetlige styringssystem (eForvaltningsforskriften, 2004, para.15). Omfang og innretning på internkontrollen skal også være tilpasset risiko (eForvaltningsforskriften, 2004, para.15). Å ta i bruk og følge anerkjente standarder nøyaktig er ikke obligatorisk, men anbefalt, i tillegg vil begrepet i forskriften "basere seg på" gjøre det mulig for lokale tilpasninger (Digdir, u.å-d). Dette vil si at kommunene vil kunne velge ut det styringssystemet som passer best for deres virksomhet så lenge de omfavner minimumskravet i eForvaltningsforskriften § 15, og følger personopplysningsloven som ble fornyet i 2018 på bakgrunn av "general data protection regulation" (GDPR). Kravene som fremgår i personopplysningsloven, er i stor grad overlappende med kravene til eForvaltningsforskriften (Digitaliseringsdirektoratet, u.å). Andre særegne lover gjelder også, samt sikkerhetsloven.

6.2 Casebeskrivelse

Som man ser i delkapittelet 6.1 finnes det ulike krav til styring i kommuner som er de kontekstuelle faktorene som påvirker caset. I denne seksjonen beskrives caset som ble diskutert i metoden. For å kunne omfatte mer enn personer og organisasjoner, ser vi på fenomen, problemer og prosesser. I vår studie er caset relatert til arbeidet med ISS i kommunen.

For å oppnå god kontroll og styring, samt tilstrekkelig sikkerhet i en virksomhet, finnes det grunnleggende aspekter med fokus på informasjonssikkerhet (Digdir, u.å-a). Disse aspektene innebærer at ledelsen har det overordnede ansvaret for at informasjonssikkerheten overholdes. Ledelsens gjennomgang bør gjennomføres, og omhandler å effektivisere og forbedre styringssystemtematikken. Roller og ansvar skal være tydelig definert og formidlet til dem det gjelder, samt at arbeidet for å opprettholde tilstrekkelig sikkerhet gjennomføres systematisk (Digdir, u.å-a). Risiko må håndteres og vurderes på en god måte og det må bygges en sterk sikkerhetskultur med riktig kompetanse. En jevnlig evaluering av arbeidet skal gjøres for å vurdere om arbeidet med informasjonssikkerhet gjennomføres i henhold til føringer som er satt, er hensiktsmessig organisert, samt at det er gjort kostnadseffektivt. God styring og kontroll bygges over tid og det vil derfor være nødvendig med kontinuerlig forbedring for å få mest mulig ut av ressursene som brukes (Digdir, u.å-a). Det som kjennetegner virksomheter som jobber helhetlig med styring og kontroll, er at de har gjenkjennbare prosesser på tvers av fagområder, har alle relevante områder inkludert, samt at ledelsen og ansatte forstår og ser informasjonssikkerhetsarbeidet i sammenhengen med styring av andre områder (Digdir, u.å-b). Mye av det som er beskrevet i dette avsnittet gjenspeiler seg også i funnene fra litteraturgjennomgangen (jfr. kap. 3) hvor ansvar og roller, kontroll, ledelse, sikkerhetskultur og kompetanse trekkes frem som viktige komponenter for ISS.

Dersom virksomheter opplever brudd på informasjonssikkerheten kan dette få konsekvenser for økonomi, leveranser, og utførelsen av oppgaver og tjenester. I tillegg kan det føre til negative konsekvenser for ansatte, innbyggere, samfunnsfunksjoner eller nasjonale sikkerhetsinteresser (Digdir, u.å-b). Ifølge direktøren i Datatilsynet, er ikke informasjonssikkerheten i kommunene god nok, og de står ovenfor store utfordringer når det kommer til informasjonssikkerheten (Datatilsynet, 2019). Økende grad av digitalisering og kommunesammenslåinger, der ulike fagsystem, kulturer, og mennesker slås sammen, kan erfaringsmessig skape store utfordringer for personvern og informasjonssikkerhet (Datatilsynet, 2019, para.4-5). I en rapport Digitaliseringsdirektoratet har laget i dialog med kommunesektorens organisasjon (KS), kommer det frem at fylkeskommuner og kommuner ikke har tilstrekkelig kontroll og styring på informasjonssikkerheten. Spesielt gjelder dette små og mellomstore kommuner (Digdir, 2020).

Små kommuner kjennetegnes ved at de over flere tiår har hatt utfordringer med reduksjon i folketallet, samtidig som de har utfordringer med å skaffe seg tilstrekkelig kompetanse på flere områder og mangel på økonomiske ressurser (Brandtzæg et al., 2019, s. 9). Små kommuner vil i årene fremover i økende grad ha utfordringer med kompetanse innenfor digitalisering, utvikling og innovasjon. Videre vil det være et økende behov for interkommunalt samarbeid hvor faste samarbeidskonstellasjoner med en felles digital infrastruktur driftes og utvikles (Brandtzæg et al., 2019, s. 11-12). Andre kjennetegn ved små og mellomstore kommuner er at disse i mindre grad har skriftlige retningslinjer for informasjonssikkerheten og mangler en utnevnt person som er fagansvarlig for informasjonssikkerheten (Digitaliseringsdirektoratet, 2020, s. 2). Videre gjennomføres det lite

kompetansehevende aktiviteter og systematiske risikovurderinger (Digitaliseringsdirektoratet, 2020, s. 11-12, 18).

Ettersom det å ha et godt styringssystem og tilstrekkelig internkontroll har hjemmel i lover, fremhever det viktigheten ved å praktisere dette. For Digitaliseringsdirektoratet er informasjonssikkerhet et viktig satsningsområde i norske kommuner, slik at digitalisering kan sikre trygge og brukervennlige tjenester for innbyggere. I tillegg finnes det ulike veiledere og verktøy for kommuner og fylkeskommuner som kan hjelpe dem i å jobbe systematisk med informasjonssikkerheten (Digdir, 2020). Basert på de generelle utfordringene som er beskrevet ovenfor, er dette noe som gjenspeiler seg i kommunene i studien, og som flere av informantene bekrefter. Dette kommer tydeligere frem videre i studien hvor forskningskontekst og casebeskrivelse blir brukt til å presentere og sammenligne funnene som fremkommer i intervjuer og dokumenter. Utfordringer og gode eksempler vil bli diskutert i diskusjonskapittelet.

7. Resultater og analyse

I dette kapittelet presenteres resultater fra analysen av empirien vi samlet inn fra informantene. Første delkapittel viser institusjonelle logikk vi identifiserte rundt arbeidet med ISS. Andre delkapittel ser arbeidet med ISS ut ifra institusjonelt arbeid i tillegg til utfordringer man møter i dette arbeidet. Kapittelet er delt inn i to deler, del én om institusjonell logikk og del to om komponentene under ISS. Hele rammeverket i Figur 4 blir ikke brukt videre, men kun utvalgte komponenter hvor vi identifiserte flest utfordringer fra vår kildedata. De ulike komponentene som vi går videre med er: revisjoner og kontroll, opplæring og sikkerhetskultur, eierskap, samt ansvar og roller.

7.1 Institusjonell logikk i arbeidet med ISS

Institusjonell logikk som teoretisk linse har gjort det mulig å identifisere årsaker til utfordringer og hvilke faktorer som former håndteringen av ISS i kommunene. Når man tar i bruk institusjonell logikk krever det at forskeren baserer sin innsikt i kildedata i form av sitater (Reay & Jones, 2016, s. 442) og derfor vil det i dette avsnittet bli presentert sitater fra informantene som informerer valg av logikkene. Selv om markedslogikk/NPM ifølge litteraturen har tatt mer over, ser vi ut ifra vår kildedata at det eksisterer andre logikker som blir brukt i kommunenes arbeid med ISS. Det var kun byråkrati- og profesjonslogikk som skilte seg ut i analysen. Det som ligger til grunn for disse logikkene blir presentert i de følgende avsnittene.

7.1.1 Byråkratilogikk

Kommunene organiseres på mange ulike måter, og i rapporten fra Digitaliseringsdirektoratet (2020) om ISS i norske kommuner, viser de til etatsmodellen eller sektormodellen som baserer seg på tradisjonell og hierarkisk organisering, men det finnes også store variasjoner i hvordan kommuner organiserer seg:

> "Kommunelovens regler om organisering åpner i utgangspunktet opp for store variasjoner i hvordan fylkeskommuner og kommuner organiserer seg. Tradisjonelt har den administrative strukturen fulgt en hierarkisk organisasjonsmodell basert på en inndeling i etater eller sektorer, ofte kalt etatsmodellen eller sektormodellen." (Digitaliseringsdirektoratet, 2020, s.7).

Den tradisjonelle organiseringen indikerer en byråkratilogikk, hvilket bygger på hierarki og kontroll. I Tabell 7 i kapittel 4.2, ble det presentert ulike kjennetegn på byråkratilogikk slik som kontroll, ansvarsroller, hierarki og sentralisert system. Disse kjennetegnene identifiserte vi hos flere av informantene, som illustreres i de kommende sitatene. Når det gjaldt IKT-samarbeidet ga en av informantene uttrykk for at det krevde tydelig styring ovenfra og ned: "Jeg tror det er lurt at de små kommunene har det enkelt når det gjelder sin internkontrollrutine og at man styrer det veldig overordnet når det er et IKT-samarbeid." (Informant E1).

Kommunedirektøren sin rolle var tydelig blant noen av informantene og denne rollen ble sett på som en nøkkelrolle og øverste ansvarlige: "Kommunedirektør er øverst ansvarlig når det gjelder dette, han er den som er virksomhetens leder og ansvarlig for alt som skjer. Avhengig av at systemeier gjør det de gjør." (Informant C2). Videre var en av logikkene til

kommunedirektøren å sørge for å delegere ansvar: “Kommunedirektør har ansvar for alt, så hans metodikk da er å delegere ansvar og tydeliggjøre for sin ledergruppe hvilke ansvar som er delegert, og så sildrer det nedover." (Informant C3). Informanten fortalte videre at sikkerhetsansvarlig ble betegnet som “kommunedirektør” innen informasjonssikkerhet og måtte hele tiden avklare saker med kommunedirektør og måtte selv vite hvilken myndighet kommunedirektøren hadde delegert til h*n, særlig om h*n ikke hadde myndighet selv.

Hierarki ble nevnt blant flere informanter og kommunedirektøren var øverste ansvarlig for sikkerheten og hadde ansvar for å delegere arbeidet:

> “Det er et hierarki, det er kommunedirektør som er overordnet ansvarlig. Mye av det overordnede ligger hos kommunedirektør, og så er mye delegert til enhetsledere. Så de har ansvar for sitt fagområde. Så skolesjef, oppvekstsjef, har ansvar for informasjonssikkerhet og personvern på sitt fagområde, blant annet gjennomføre internkontroll, ROS, DPIA, de har ansvaret for seg selv egentlig. Og så har de meg, som en intern masekråke som etterspør om de har husket på å gjøre det.” (Informant G1).

I intervjuene uttrykte en av informantene at noe av fremtiden lå i å styre sentralt ettersom de mindre kommunene ofte har problemer med å gjøre mye av arbeidet med ISS selv, da de ikke har ressurser til å etterleve personvern og sikre IT. På en annen side kunne det være utfordrende å styre så overordnet, ettersom det kunne hindre folk i å ta ordentlig eierskap til det:

> “Det arbeidet med personvern bør etter min mening ligge i forvaltningen, som da er en fra hver kommune rigget via [IKT-samarbeid]. Det er også nettopp dette som er litt negativt ved at hver kommune får litt avstand til det, kanskje ikke tar helt eierskap til det med en gang. Men samtidig er det litt fremtiden også, fordi de små kommunene de klarer ikke dette her alene tror jeg, de klarer ikke ha brannmurer, masse folk som jobber med GDPR. Er ganske trang økonomi, tror sentralisering for små kommuner er positivt.” (Informant E1).

En av informantene uttrykte at de stilte spørsmål og måtte kontrollere systemeierne: "Jeg opplever hvert fall i liten grad at det er vi som sitter sentralt som blir fulgt opp av systemeiere, det er nok mer motsatt, at det er vi som stiller spørsmål og kontrollerer litt hvordan de forvalter systemene sine." (Informant A1).

Analysen viser at flere av informantene etterlyste tilstrekkelig oppmerksomhet fra toppledelsen og at det særlig var utfordrende å få oppmerksomheten til kommunedirektøren:

> “Kunne ønske at den oppmerksomheten hos kommunedirektøren etterspør den, det kommunedirektøren vil ha det får han. Bruker tid på det istedenfor noe annet. Men når kommunedirektøren vil ha noe annet så er det det vi må bruke tiden på. Kommunedirektør og assisterende her hos oss, er nøye på hva vi får bry lederen med. Så det er en frustrerende flink portvakt […]. Når kommunedirektøren ikke interesserer seg for det, får man ikke gjort det” (Informant D1).

Fra datamaterialet har vi gjenkjent byråkratilogikk blant flere av informantene. Ettersom ISS baserer seg på blant annet å ha tydelige ledere som setter føringer nedover, sentral styring, tydelige roller og hierarki, viser dette til byråkratilogikk. Noen mente at man var avhengig av en byråkratisk styring for å få til arbeidet med ISS, særlig når det kom til de små kommunene. På en annen side ble dette også sett på som utfordrende da man kunne forårsake at virksomhetene fikk mer avstand til det. I tilfeller var det frustrerende med en slik logikk,

hvert fall når kommunedirektøren ikke interesserte seg for arbeidet med informasjonssikkerhet. Dette viser at byråkratilogikk kan påvirke arbeidet med ISS i både positiv og negativ forstand.

7.1.2 Profesjonslogikk

En tydelig logikk vi identifiserte blant flere av informantene var profesjonslogikk. Ettersom arbeidet med ISS også omfavner kommunens virksomheter, vil man møte mange personer med ulike profesjoner og bakgrunner. Flere av informantene uttrykte at det var enklere å arbeide med sikkerhet innen helse og omsorg. Dette fordi profesjoner i denne virksomheten hadde innarbeidet sikkerhet i arbeidskulturen, samt slike verdier gjennom deres utdanning. Kulturelle forskjeller rundt om i kommunen ble nevnt som en faktor som kunne forklare hvorfor noen har større bevissthet rundt informasjonssikkerhet enn andre:

> "Det er noen kulturelle forskjeller rundt om i kommunen. Det vi opplever er at de som hører til helse og velferd, de har en høy bevissthet når det gjelder informasjonssikkerhet og personvern, de har det med seg fra utdanningen sin, de er vant til å håndtere sensitive personopplysninger." (Informant A1).

> "Sykepleiere melder avvik på seg selv, "i dag gjorde jeg feil på jobb", eller kommer på jobb og ser at kollegaene har gjort feil, er en helt naturlig del av hverdagen. Det handler om kultur, men også grunnleggende forståelse i bunnen." (Informant F1).

> "Alle som jobber i helse, har fra sin utdannelse, og gjennom autorisasjoner, i ryggmargen, om taushetsplikt. Den respekten for andre mennesker. Det glipper jo der og, men kulturen i sektoren er forskjellig i forhold til personopplysninger. Det har gått mellom mange, mange år, en respekt for journaler. Også er det etter hvert en bedre kultur for avviksmeldinger, for det har de jobbet veldig lenge med i helsesektoren." (Informant A2).

Analysen viser at personer som jobber innenfor helse har en høyere bevissthet rundt informasjonssikkerhet. Dette har gjort arbeidet med ISS enklere mot gruppene innenfor helse og omsorg: "Prinsippene om kontinuerlig forbedring er enklere å jobbe inn hos dem enn hos andre for eksempel." (Informant F1). De har også bedre sikkerhetskultur: "Det er en god sikkerhetskultur på helseopplysninger på helse og omsorg. Og det gjør at de trenger ikke å løfte denne fanen så høyt hele tiden." (Informant D1). Dette var det flere informanter som sa seg enige i: "HSO (helse og omsorg), har større kultur for rutiner og prosedyrer på plass, og er mer opptatt av avvik og avviksmeldinger, enn andre kommunale områder." (Informant C2).

Videre ble det rapportert flere avvik blant helse og omsorg enn de øvrige virksomhetene i kommunene:

> "Kan ta et eksempel fra helse, de er veldig familiære med avvik, og har vært det gjennom mange år, fordi det grodde frem på legemiddelhåndtering. Sånn at det ligger i deres natur og kultur bedre enn hos andre." (Informant C3).

Selv om helse og omsorg var enklere å arbeide med når det kom til ISS, opplevde flere av informantene utfordringer med andre. En av informantene opplevde at det var tydelig gnisninger mellom IKT-avdelingen og administrasjonen, da IKT hadde et teknisk tankesett og manglet det medmenneskelige, noe som viser at det eksisterer tydelig motstridende syn,

hvilket relaterer til motstridende logikker. Dette var med på å gjøre arbeidet med ISS vanskelig:

> "Planen er å drive med interne revisjoner. Vi driver og tester ut noen piloter nå, så på et eller annet tidspunkt vil nok det være en del. Vi vil nok få det til på enhetene i kommune tenker jeg, men slik jeg ser det i dag tror jeg det blir vanskelig å få det til opp mot IKT avdelingen. Vi kan bli gode på internkontroll på informasjonssikkerhet ute på de ulike enhetene, det skal vi klare, men akkurat opp mot IKT-avdelingen så er jeg litt usikker på veien og prosessen der." (Informant F1).

> "Blir mye på det tekniske, men samtidig er det de som sitter på kompetansen på å gi opplæring på fagsystemene, ofte opp mot sluttbrukere hos de ulike enhetene. Jeg tenker de er gode på det tekniske, men dårlig på det medmenneskelige og det organisatoriske. De er sikkert skinnsykt flinke med en gang å finne feil på en kode eller dimensjonere server, ting som ikke jeg kan noe om, er de sikkert gode på, men det er en del andre ting som også skal til." (Informant F1).

Skole og oppvekst var en av virksomhetene som ble nevnt av informantene at det var flest utfordringer å jobbe med når det kom til arbeidet med ISS. Empirien baserer seg på informantenes opplevelser av en annen gruppe mennesker og deres logikker. Kultur og verdier blir mye diskutert om akkurat denne profesjonsgruppen, og som informantene utrykker, støtter ikke deres logikk arbeidet med ISS like godt sammenliknet med helse og omsorg:

"Innen oppvekst er det litt annerledes. Hadde tilsyn fra datatilsynet på en skole i 2014, måtte jobbe litt jevnt for å få de digitaliseringsrådgiverne innen oppvekst til å forstå poenget." (Informant D1).

> "I oppvekst, der er det veldig mye myke verdier, og de har ikke den sikkerhetstankegangen. Kulturen i oppvekst er at de bruker det de får tak i av verktøy og lærerne er kreative, og noen er veldig ivrige, en kultur hvor det er hundre i innsats og null i vurderinger." (Informant A2).

> "Sykehusene begynner å hjelpe, at det er greit å melde avvik fordi det kan redde liv. Og at det blir en kultur hvor man ser på det som positivt. Det er litt umodent når det kommer til oppvekst" (Informant A2).

> "Innenfor oppvekst og skoler, der er det ikke så modent som helse og velferd, og dessuten er den preget av litt mer mangfold. Tenker nok at mange lærere og skoleledere mener at "vi står fritt til å velge hvilke apper og pedagogiske verktøy vi skal bruke på skolen vår". Men dette finnes ikke på sykehjem og sykehus, de går helt i takt, de er en homogen gruppe, mens skolesiden er mer sånn "la de tusen blomster blomstre". Det fører jo til at, det er kanskje i denne sektoren vi ser mest utfordringer i forhold til informasjonssikkerhet og personopplysninger." (Informant A1).

> "Skole, de er våkne når det skjer noe for eksempel i Bergen og Oslo, og nyhetssaker og sånn. De tar det litt som det kommer. Samtidig håndterer skole veldig mye personsensitiv informasjon, og det er det jeg kjenner på som utfordrende. Det er der jeg har mest fokus selv da, og det er jo ikke bare hvor lagrer vi data og hvordan håndterer vi det, men hva har vi lov til å lagre. Det er vanskelig spesielt innenfor oppvekst." (Informant G1).

Basert på analysen kan man se at profesjonslogikken som eksisterer innen virksomhetsområdet helse og omsorg er enklere å jobbe med, enn de som har

profesjonslogikk innen skole og oppvekst når det kommer til arbeidet med ISS. Utfra analyse av kildedata fra flere informanter, fant vi ulike trekk som støtter arbeidet med ISS, hvilket vi har valgt å kalle ISS-logikk. Denne logikken bygger på samarbeid på tvers, deling av informasjon, positiv assosiasjon til avvik, kontroll og revisjon. De ulike verdiene som ligger til grunn er basert på antall ganger de har blitt sitert av informantene, basert på analyse i NVivo. Dette er med andre ord symbolske og materialistiske elementer som blir gjentatt flere ganger og som har en positiv innvirkning på arbeidet med ISS. Ettersom dette er punkter som også passer under ISS-komponentene i delkapittel 7.2 har vi ikke tatt med alle sitatene her som viser grunnlaget for logikken, da dette ville resultert i for mye gjentakelser. Vi ønsker derimot å gi noen eksempler på sitater som viser grunnlaget for logikken ettersom dette blir betegnet som viktig av Reay og Jones (2016) (s.443) for å overbevise leseren om hvordan vi kom frem til logikken.

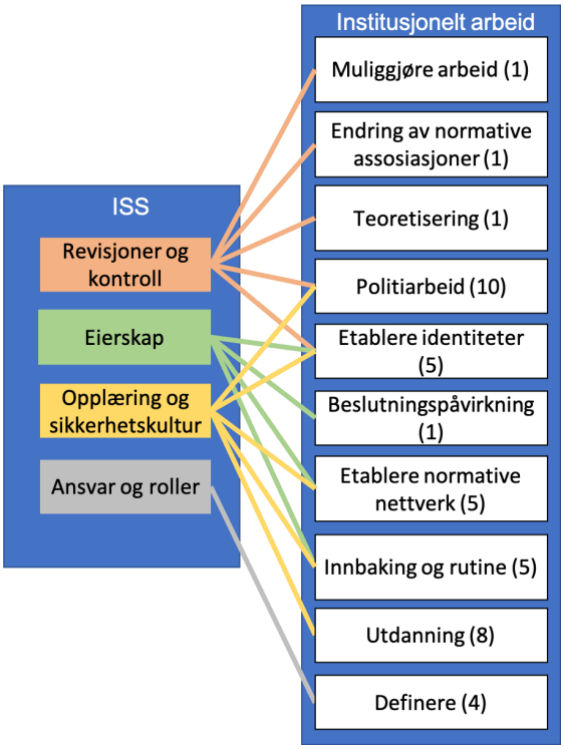
Tabell 12: Eksempler på sitater som viser grunnlag for logikk

Symbolske/materialistiske elementer	**Sitater**
Samarbeid på tvers	"[…] Så er de med i et nettverk som jobber med informasjonssikkerhet på tvers."
Positiv assosiasjon til avvik	"Vi tenker som så at jo flere avvik man får inn, det tyder egentlig på god bevissthet og god holdning og en vilje til å forbedre seg. Så vi bruker det som et forbedringsverktøy."
Kontroll og revisjon	"Vi er ute hos 3-4 virksomheter i året og har interne sikkerhetsrevisjoner. Vi ser hvordan de jobber, opplæring av folkene, hvordan er tilgang til byggene her, melder dere noen avvik, risiko osv. Da har vi fått ringen litt slutta."
Deling av informasjon	"Jeg har jobbet mye i det private, ser at mange kommuner sitter hver for seg, det med å utveksle erfaring i større grad tror jeg er veldig viktig."

I neste delkapittel vil vi ta for oss ulike hovedkomponenter av ISS, hvordan kommunene vi har data fra arbeider med dette og utfordringene de møter.

7.2 Informasjonssikkerhetsstyring og ISS

Som nevnt tidligere finnes det mange ulike komponenter som defineres som viktige hovedkomponenter av ISS. De følgende komponentene blir presentert; revisjoner og kontroll, eierskap, opplæring og sikkerhetskultur, samt ansvar og roller. Institusjonelt arbeid blir brukt til å forklare hvordan kommuner jobber med disse komponentene, samt utfordringene de møter. Figur 7 viser de ulike hovedkomponentene av ISS som dette kapittelet er strukturert etter, komponentenes kobling med type institusjonelt arbeid og antall sitater markert med tall i parentes. Vi har kun basert oss på de ulike typene institusjonelt arbeid fra Lawrence & Suddaby (2006) som illustreres i Tabell 8 i delkapittel 4.4. I Figur 7 mangler også institusjonelt arbeid som handlet om å *forhindre institusjoner*. De typene institusjonelt arbeid vi identifiserte i datamaterialet handlet derfor kun om å *ivareta* eller *skape institusjoner.* Som man kan se i Figur 7, mangler det noen typer institusjonelt arbeid. I vår kildedata under *skape institusjoner* fant vi ingen indikasjoner på arbeid som omhandlet *opptjening* eller *mimikk.* Under *ivareta* institusjoner fant vi ikke institusjonelt arbeid relatert til *avskrekking*, *valorisere og demonisere* eller *mytologisering*.

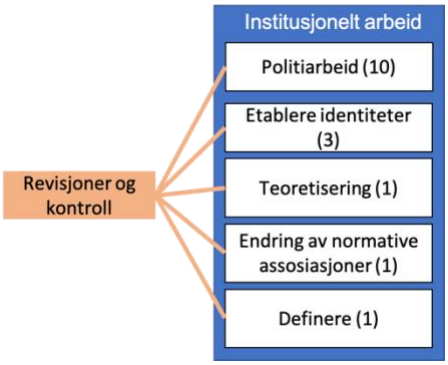


Figur 7: Oversikt over komponenter i sammenheng med institusjonelt arbeid

7.2.1 Revisjoner og kontroll

Revisjoner og kontroll er en viktig komponent av ISS. I rapporten fra Digitaliseringsdirektoratet kom det frem at små og mellomstore kommuner i liten grad gjennomførte revisjoner og kontroll for å forbedre ISS: "Kommuner har i mindre grad enn fylkeskommuner evaluert, forbedret eller fornyet styringssystemet for informasjonssikkerhet. Få fylkeskommuner og kommuner oppgir at de har rapportert erfaringer fra øvelser til bruk i risikovurderinger og/eller forbedring av informasjonssikkerheten." (Digitaliseringsdirektoratet, 2020, s.2). Dette blir gjort i mindre grad i de små og mellomstore kommunene enn i fylkeskommuner: "Når det gjelder kommunene, oppga 52,3 %, 64,4 %, og 61,2 % at de har gjort tilsvarende i henholdsvis 2018, 2019 og 2020." (Digitaliseringsdirektoratet, 2020, s.15).

Derfor var det interessant å finne ut om dette stemte overens med våre funn og i tillegg finne ut hvorfor det var slik. I dette avsnittet presenteres resultater fra analysen som viser hvordan det jobbes med revisjoner og kontroll, samt utfordringer. Innenfor institusjonelt arbeid baserte revisjoner og kontroll seg mest på **politiarbeid**. Figur 8 viser dataene vi kategoriserte som institusjonelt arbeid under revisjoner og kontroll.



Figur 8: Data kategorisert som institusjonelt arbeid under revisjoner og kontroll

Politiarbeid i form av revisjoner og kontroll ble sett på som viktig ettersom man kunne få tilbakemelding på om virksomhetene gjorde det de skulle i forhold til arbeidet med informasjonssikkerhet. Denne typen arbeid ble praktisert jevnlig i noen kommuner og årlig hos andre, flere kommuner så også på avvik som en viktig del av dette arbeidet:

> "Vi er ute hos 3-4 virksomheter i året og har interne sikkerhetsrevisjoner. Vi ser hvordan de jobber, opplæring av folkene, hvordan er tilgang til byggene her, melder dere noen avvik, risiko osv. Da har vi fått ringen litt slutta, med at vi ikke bare har styrende dokumenter og rutiner og hvordan det skal gjøres, men vi kontrollerer også at virksomheter gjør det de skal." (Informant A1).

Blant noen av informantene var det å revidere og analysere avvik sett på som nyttig i forhold til arbeidet med revisjoner og kontroll:

> "Vi tenker som så at jo flere avvik man får inn, det tyder egentlig på god bevissthet og god holdning og en vilje til å forbedre seg. Så vi bruker det som et forbedringsverktøy. Når man ser det er noen avdelinger som aldri melder et eneste avvik, så bør vi jo jobbe litt der. Men det får vi opp statistikk på. Ser hvem som melder mye eller lite […]. I november var det 413 avvik totalt på kommunen, ønsker at det skal være høyt for å få til forbedringer. Hadde møte med teknisk avdeling og de hadde veldig klare målsettinger om høyt antall på avvik, for de ser det som en god mulighet til å utvikle seg både internt og for kommunen" (Informant H1).

Å utøve politiarbeid gjorde det mulig å hele tiden ha kontroll på tilstanden til de ulike virksomhetene, dette var videre med på å skape bevissthet rundt avvik og informasjonssikkerhet:

> "Vi har en virksomhetsplan og rapportering, sjekklister som alle må svare på. Informasjonssikkerhet og personvern, som enhetene har en oppdatert oversikt over, behandling av personopplysninger. Da må de gjøre en bevisst handling og det er også sånn som internkontroll, bruke avviksmeldinger, bevisstgjøre dem gjevt og trutt, ikke noe som bare ligger i en skuff." (Informant H2**)**.

Det varierte fra kommune til kommune hvor ofte de gjennomførte revisjoner og kontroll. Flere hadde en årlig gjennomgang for å undersøke hvordan de lå an:

> "Det er jo et umettelig marked for opplæring, kompetanseheving. Hvert år leverer alle inn egenmelding som en del av årsstatusen fra virksomheten. Det er det [personvernombud] som har samlet inn. Da er det et spørreskjema som må fylles ut, enkle ting som, har alle ansatte skrevet under taushetserklæring, har du oppdatert deg på styrende dokumenter, har dere gjort risikoanalyse osv. Da får man jo en indikasjon

> på status i virksomheten. Ut ifra dette får vi et inntrykk hvor det er størst risiko for stor skade til enhver tid. Også går vi etter der det er størst risiko for skade." (Informant A2).

To av kommunene fortalte at de hadde en årlig gjennomgang av informasjonssikkerheten: "Se om det jeg har satt i gang blir gjennomført og følge opp en årlig sikkerhetsgjennomgang, og kikke litt i avvikssystemet, og se at det virker." (Informant J1). "Kommunedirektørens ledergruppe har en årlig gjennomgang av informasjonssikkerhet. Gjennomgangen ser blant annet på avvik som er meldt i Compilo, egenkontroller, endringer i trusselbilde og ressurser for å ivareta internkontroll og informasjonssikkerhet." (Revisjon Sandnes kommune, 2019). Selv om noen av informantene fikk dette til, ble det blant noen uttrykt at mangel på ressurser hindret dem fra å gjennomføre revisjoner selv om de ønsket å prioritere det:

> "Vi hadde en ambisjon om å drive revisjoner, men kom aldri så langt. Når kommunedirektøren ikke interesserer seg for det, får man ikke gjort det. Hadde en intensjon om at gruppen med personvern og sikkerhet kunne vært ute og revidert hverandre, men hverdagen strekker ikke til. Det blir ikke viktig nok til at vi klarer å prioritere." (Informant D1).

Vi spurte kommunene om de kunne kontrollere om ansatte i kommunen hadde gjennomført opplæring. I en av kommunene gjennomførte de kontroll hvor de brukte statistikken fra KS læring: "Via KS læring, hver enkelt leder kan følge opp på det" (Informant H1). Hos en av kommunene var ikke avvikssystemet tatt i bruk for hele organisasjonen. Informanten hadde derfor en jobb å gjøre med å få dette til å bli brukt mer aktivt:

> "Vi har et avvikssystem, men det er ikke i bruk for hele organisasjonen enda, har vært i den ene kommunen i samarbeid, men ikke her. Vi har nylig begynt å bruke det på pleie og omsorg, og så har ikke hele organisasjonen tatt det i bruk, tenke jeg skulle mase litt om det, det er og en del av min rolle." (Informant G1).

Selv om institusjonelt arbeid i form av politiarbeid ble praktisert i flere av kommunene fantes det også variasjoner. Det var tilfeller der man heller baserte seg på tillit: "Det er i veldig stor grad tillitsbasert, eller så må vi ut å kjøre en form for undersøkelse eller revisjon." (Informant D1). Utfordringer med å revidere og analysere ble også nevnt blant flere av informantene, særlig når det kom til avvik. I et av tilfellen ble avvik holdt unna fordi de som kontrollerte ble oppfattet av andre som "skumle": "Plutselig blir avvik hold langt unna meg fordi jeg blir skummel, er en vanskelig balansegang." (Informant G1). Derfor var det viktig å jobbe med å endre dette synet og skape nye idealer hvor man ser forbedringsmuligheter og avvik som noe positivt. Å jobbe med å skape nye idealer og identiteter relaterer til **etablere identiteter** innen institusjonelt arbeid. I kombinasjon med politiarbeid førte dette til å skape andre holdninger hos blant annet lederne i kommunens virksomheter og de ble mer bevisste og delaktig i arbeidet med ISS:

> "De første som fikk besøk av oss syntes det var litt skummelt, men vi prøver å si at dette er forbedringsarbeid, og vi er ikke ute etter å finne feil, men å finne forbedringsmuligheter og komme med råd for hvordan man kan gjøre arbeidet sikrere og bedre. De siste revisjonene vi har gjennomført, har lederne vi har intervjuet, uttrykt at det er bra å få drahjelp til dette feltet." (Informant A1).

Særlig ble avvik ofte oppfattet som noe negativt og det var viktig å endre dette synet. En måte å gjøre dette på var å kommunisere at avvik handlet om forbedringsarbeid. Denne typen arbeid henger sammen med **teoretisering** innenfor institusjonelt arbeid som er med på å

endre oppfatninger og assosiasjoner til konsepter eller praksis. Å endre synet på en praksis slik som synet på avvik, henger også sammen med **endring av normative assosiasjoner**:

> "Mange har hatt en litt negativ holdning, avvik er ikke et positivt ladet ord. Men vi prøver å kommunisere at det egentlig er et forbedringsverktøy, og det er aldri ment for å henge ut noen, og de blir applaudert de som melder avvik. Det er det vi forsøker å sende ut" (Informant H1).

Det var noen kommuner som møtte på utfordringer med å utøve slikt arbeid og få til den nødvendige kulturendringen:

> "Jeg tror den største utfordringen handler om å få endret kulturen slik at dette blir oppfattet hele veien som noe positivt, at det ikke er noe sladring. Da blir det jo sånn at et avvik som ikke er registrert det har jo ikke skjedd. Da har vi jo ikke noe kontroll på dem." (Informant A1).

En av informantene uttrykte at ansatte i virksomhetene opplevde at det var vanskelig å skille mellom avvik og uønskede hendelser. Et eksempel på en uønsket hendelse ble definert som for eksempel "eldre som faller på sykehjem" (Informant G1). Avvik ble definert som "når en avviker fra rutiner og retningslinjer" (Informant G1). Dette førte til at de ansatte rapporterte uønskede hendelser som ikke omhandlet informasjonssikkerhet under denne kategorien, og det var vanskelig å få kontroll, føre statistikk og historikk til noe nyttig i det videre arbeidet:

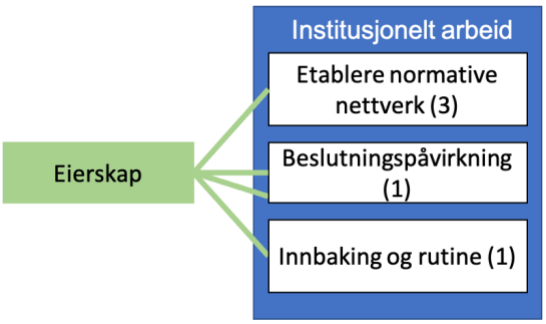
> "Jeg blir litt forvirret av det med avvik, for jeg mener at et avvik er når man avviker fra retningslinjer og rutiner, men en uønska hendelse er noe helt annet. Jeg hadde ønsket av vi skilte på det, det er det jo ingen som gjør. Det gjør det litt vanskelig å snakke om avvik […]. Hendelses- og avvikssystem er jo ett og samme, og jeg tror det er mest uønskede hendelser som er meldt fra helse, og da er det knyttet mot brukere tror jeg, veldig lite på informasjonssikkerhet. Man skjønner ikke helt forskjellen og derfor driver jeg og maser om at det er to forskjellige ting." (Informant G1).

En av kommunene hadde bygd opp sitt ISS-system på anerkjente ISO-standarder og deres internkontrollsystem var basert på dette. Regelstrukturer og standarder som ISO, henger sammen med **definere** innenfor institusjonelt arbeid: "Dette systemet er basert på ISO-standarden, hele internkontrollsystemet er basert på det" (Informant H1).

I dette delkapittelet har vi sett på hvordan kommunene vi intervjuet jobbet med revisjoner og kontroll, samt utfordringer rundt dette arbeidet. I neste delkapittel presenteres funnene relatert til eierskap som er en viktig faktor for å få flere med på arbeidet med informasjonssikkerhet og øke bevisstheten rundt dette arbeidet.

7.2.2 Eierskap

Eierskap handler om å ta eierskap til arbeidet ved at man involverer flere personer i å utforme retningslinjer og ISS. Vi identifiserte flere ulike typer institusjonelt arbeid som var med på å fremme eierskap i arbeidet med ISS. Hvor **etablere normative nettverk** som handler om å skape interorganisatoriske nettverk på tvers av områder og ved siden av eksisterende strukturer blir sett på som et av de viktigste funnene, illustrert i Figur 9.



Figur 9: Data kategorisert som institusjonelt arbeid under eierskap

Funn viser at det var viktig å få alle i kommunesamarbeidet til å delta i arbeidet med å utforme planer og retningslinjer for ISS, og at dette var en forutsetning for å lykkes. Det var også viktig å få med alle kommunens virksomheter i dette arbeidet. Dette har vi relatert til **etablere normative nettverk** innen institusjonelt arbeid: "Jeg håper at vi involverer alle sammen fordi det har såpass stor verdi og er kompetansebyggende å jobbe med det." (Informant G1).

Et nettverk var også sett på som en viktig nøkkel i arbeidet med ISS. I tillegg støttet nettverket arbeidet med ISS på tvers av virksomhetene og sikret godt eierskap:

> "Hadde ikke vært mulig uten det nettverket. Skjer det noe innenfor oppvekst, diskuterer i forhold til oppvekst, har de representanter, oppvekst kjenner veldig på utfordringer i forhold til informasjonssikkerhet og personvern, har jo tatt de inn i dette arbeidet, og bruker de ikke bare i nettverket, men at de har mye kunnskap, får mye innsikt i problemstillingene." (Informant H1).

I dette nettverket hadde en av kommunene jevnlige møter med kommunedirektørens gruppe og nettverksmøter med de ulike virksomhetslederne. Ettersom disse møtene var såpass jevnlig kan det betegnes som **innbaking og rutine** innenfor institusjonelt arbeid, ettersom denne typen arbeid handler om å repetere praksiser jevnlig slik at det blir en rutine:

> "Vi har ledelsens gjennomgang for kommunedirektørens stab, og så har vi et nettverk, der jeg har med meg representanter, stor sett avdelingsleder eller enhetsleder, så er de med i et nettverk som jobber med informasjonssikkerhet på tvers. Har møte 1 gang i måneden, i starten hadde gjennomgang med kommunedirektørens gruppe, da skal kontaktene på områdene kjøre en ledelsens gjennomgang for eksempel innenfor oppvekst, helse og samfunn. Tar ikke kopi av min presentasjon, men lager en ledelsesgjennomgang som treffer innenfor deres område. Og da treffer man lederen. Så er det ledere som må få dette videre ned til ansatte." (Informant H1).

Nettverket gjorde det også mulig å få økt bevissthet ut i kommunen. I kombinasjon med **politiarbeid** skapte det en struktur som fungerte godt i arbeidet med ISS:

> "Jeg føler at strukturen vi har bygd opp fungerer, har prosedyreverktøy, avvikshåndtering, har definert roller, og nettverket. Det fungerer, men kan alltid bli bedre, men merker at bevisstheten øker, får økt bevissthet ut i kommunen. Men det må jobbes med kontinuerlig." (Informant H1).

Vi spurte en av informantene hvorvidt direktorater som kommer med anbefalinger om ISS hadde en innvirkning på hva som blir prioritert i kommunen. Svaret var at de kun hadde ressurser til det som må gjøres og da ble det som bør gjøres satt litt på sidelinjen. Ettersom veiledninger og retningslinjer som er utformet av direktoratene blir sett på som noe som bør

gjøres vil det ikke bli avsatt penger til det uten at det blir definert som skal: "Når de lager veiledninger, retningslinjer, pålegg, osv. Så blir ordet skal byttet ut med bør (Informant A2). Videre vil pengene forsvinne så fort man har endret skal til bør igjen: "Da er det jo sånn at når en kommune får et pålegg og det står skal, så koster det kanskje en million kroner. I det øyeblikket man bytter ut skal til bør, så forsvinner de pengene fra budsjettet" (Informant A2). På bakgrunn av dette uttrykte informanten at man var avhengig av at kommunedirektøren og kommuneledelsen var supersupporter for informasjonssikkerhet og på den måten tok et eierskap til arbeidet med ISS.

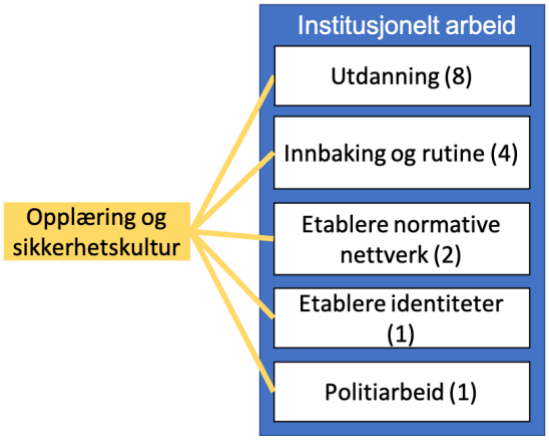
Vi observerte at i kommunesamarbeidet til en av kommunene, kjørte de en mer sentralisert tilnærming til styring enn i andre kommuner. Informanten uttrykte at kommunedirektørene i små kommuner ønsket at de skulle gjøre alt arbeidet med ISS: "Helt overordnete liksom, hva gjør [IKT-samarbeid] og hva gjør kommunene. Styringen på det, der er det veldig mange forskjellige meninger. Kommunedirektører i små kommuner ønsker at [IKT-samarbeid] skal gjøre alt." (Informant E1). I tillegg hadde de en politikk i kommunesamarbeidet som fremmet en sentralisert tilnærming til styring, hvilket informanten ikke var helt enig i at var den beste måten å styre på:

> "Ja, det er sånn de har politikk på en måte. Om det er innafor loven eller ikke vil tiden vise. Og datatilsynet og hva de mener. Men styringsdokumenter har vi ikke mange av her, er et overordnet styringsdokument som er debattert veldig også på ting". (Informant E1).

Styringsdokumenter skal spesifisere hvordan arbeidet med sikkerhetskultur og opplæring bør gjennomføres hvilket leder oss til neste delkapittel om opplæring og sikkerhetskultur.

7.2.3 Opplæring og sikkerhetskultur

Opplæring og sikkerhetskultur er viktig for å få til et godt arbeid innenfor ISS. Det var flere typer institusjonelt arbeid vi identifiserte i analysen når det kom til opplæring og sikkerhetskultur, hvor **utdanning** var den som kom mest frem. **Utdanning** handler om å utdanne aktører slik at de støtter den nye institusjonen. Figur 10 viser en oversikt over institusjonelt arbeid i relasjon til opplæring og sikkerhetskultur



Figur 10: Data kategorisert som institusjonelt arbeid under opplæring og sikkerhetskultur

I rapporten fra Digitaliseringsdirektoratet (2020) kommer det frem at opplæring og sikkerhetskultur er viktig i arbeidet med ISS: "Manglende kompetanse og forståelse hos både

medarbeidere og ledere, samt manglende kultur, utgjør hindringer i forbindelse med informasjonssikkerhet. Dette indikerer at fylkeskommuner og kommuner ikke i tilstrekkelig grad arbeider med kompetanseutvikling og sikkerhetskultur." (Digitaliseringsdirektoratet, 2020, s.3). Videre er det: "Essensielt at noen oppdager hendelser som oppstår og at man har ressurser og kompetanse til å håndtere dem. Kompetanseheving knyttet til informasjonssikkerhet er nødvendig og det er viktig at kompetansen heves i alle enheter." (NorSIS, u.å, s.29). Opplæring er også en del av **utdanning** innen institusjonelt arbeid og vi fant ulike måter å gjøre dette på, samt utfordringer med dette arbeidet som blir presentert i de neste avsnittene.

I likhet med det som fremgår i rapporten fra Digitaliseringsdirektoratet (2020), ble opplæring sett på som viktig blant informantene i å støtte arbeidet med ISS. De uttrykte at de måtte fokusere på å jobbe med opplæring over tid for å skape kulturendring: "Vi må tenke aktiv læring, jobbe med det over tid." (Informant C1). I en av kommunene, nevner begge informantene at opplæring kan føre til kulturendring og kulturbygging:

> "Veiledning og kurs, og da blir det etter hvert sånn at det blir en kulturendring. Plutselig blir det sånn "oi, kan vi ikke gjøre det sånn, hvordan skal vi gjøre det da?" og så blir det snakk på lærerværelset for eksempel. Og da får man litt den kulturendringen til." (Informant A2).

En av informantene ønsket å jevnlige snakke om informasjonssikkerhet hos de ulike virksomhetene. Således er dette en måte å både drive **utdanning** på, men også skape rutine **innbaking og rutine**, samt nye identiteter i form av **etablere identiteter** innen institusjonelt arbeid:

"Det å få inn meg som snakker litt om informasjonssikkerhet, hvordan gjør vi det i praksis, sånn skal vi ha det hos oss typ, så det er jo også en sånn kulturbygging." (Informant A2). I tillegg kan man kontrollere om ansatte har gjennomført opplæringen noe som kan relateres til **politiarbeid:**

> "Når man da gjennomfører et sånn kurs, for det er faktisk blitt gitt god opplæring i hva er gjeldene sikkerhetsinstruks, så skjer det noe begge veier. Det ene er at kommunen vet at du kan ikke komme etterpå å si at du ikke har fått opplæring eller ikke var klar over det. Fordi det er dokumentert at du har fått opplæring i det." (Informant A2).

Å utøve slikt arbeid krever gode rutiner ettersom kommunene har så mange nyansatte hvert år: "Det er ikke bare å gi en opplæring, og tenke at nå har vi gjort det. Det kommer jo mange hundre nyansatte hvert år og folk går ut, så må ha gode rutiner og kultur for å forvalte dette." (Informant A1). I Sandnes kommune sin revisjon av ISS (2019), henvises det til at de har en informasjonssikkerhetskoordinator med ansvar for å samordne og koordinere ulike tiltak: "Sørge for gjennomføring av opplærings- og motivasjonstiltak for å ivareta informasjonssikkerhet." (s.36). I tillegg var det påpekt at rollene som informasjonssikkerhetskoordinator og IT-ansvarlig skulle delta jevnlig i faglige forumer som en del av kunnskapsbyggingen som kan knyttes til både **utdanning** og **innbaking og rutine** innen institusjonelt arbeid, ettersom dette skulle gjøres jevnlig: "Delta i faglige forum og samarbeide med andre virksomheter for å opprettholde og øke kunnskapen knyttet til informasjonssikkerhetsarbeid, og dele denne med organisasjonen." (Revisjon Sandnes kommune, 2019, s.36).

En av informantene uttrykte at de fikk en push til å begynne med opplæring og sikkerhetskultur som følge av angrepet som skjedde i Østre Toten. Derfor startet de opp en

gruppe som skulle jobbe med sikkerhetskultur hvilket kan relateres til **etablere normative nettverk** ettersom det er en koordinering av ulike faggrupper på tvers som jobber felles mot en bedre sikkerhetskultur:

> "Nei, ikke jevnlig, men satt i gang som en bakgrunn fra det som skjedde på Østre Toten. Flere som er utsatt for hacking, har satt inn en gruppe som jobber med sikkerhetskultur, som består av meg, IT-leder, rådgiver og en leder fra kultur, idrett og fritid." (Informant C2).

At hendelser slik som i Østre Toten økte fokuset på informasjonssikkerhet og styring bekreftes også av andre: "Får på en måte drahjelp når det skjer et angrep. Den store kulturbyggingen er jo at vi er sårbare." (Informant A2). I tillegg ønsket en av kommunene å gjøre sikkerhet til et tema på kommunedirektørens møter, slik at seksjonsleder tok det videre ned til sin organisasjon for å bygge kompetanse og ta de rette valgene. Dette arbeidet relateres til både **utdanning** og **innbaking og rutine**. Deltakelse i et velferdsteknologiprosjekt hvor et eksternt konsulentselskap hadde en viktig rolle opp mot en av kommunene bidro med økt bevissthet rundt informasjonssikkerhet. Konsulentselskapet hadde en rolle med **utdanning** samt bake inn opplæring på informasjonssikkerhet som en del av arbeidshverdagen som kan defineres som **innbaking og rutine.**
Velferdsteknologiprosjektet betegnes som **normative nettverk** ettersom det involverte flere ulike parter på tvers til å samarbeide om informasjonssikkerheten. Dette førte til at informasjonssikkerhet kom høyere opp på agendaen:

> "[Konsulentselskap] jobber mye mot oss, har masse verktøy, og nå har det endelig blitt satt på agendaen der og, som del av den opplæringen. Og mine opplevelser er at våre også snur seg mer til meg og sier "men de sier jo det du har masa om", plutselig så skjønner de at vi skal gjennomføre ROS analyser og DPIA." (Informant G1).

Selv om opplæring blir sett på som viktig for å lykkes har det også oppstått utfordringer rundt dette, som for eksempel at opplæringsprogrammene ikke fungerer bra nok. Tall fra rapporten fra Digitaliseringsdirektoratet (2020) viser at opplæring og bevisstgjøring ikke blir gjennomført i stor nok grad hos små og mellomstore kommuner og kun 34% av de små og 46.9% av de mellomstore utfører slike kompetansehevende aktiviteter (s.20). En av informantene bekreftet at dette er en utfordring og et aktuelt problem som førte til at man ikke hadde god nok kompetanse om informasjonssikkerhet hos de ulike ledernivåene: "Nok kompetanse i organisasjonen på alle ledernivå og forståelse, henger jo sammen med kompetanse." (Informant G1).

Svar fra informantene viser at institusjonelt arbeid i form av **utdanning** innen opplæring og sikkerhetskultur ikke alltid er lett å gjennomføre. Blant problemer som oppstod var at nyansatte ikke fikk tilstrekkelig opplæring og ikke fikk tid til å sette seg inn i oppgavene:

> "Vi har opplæringsprogram for nyansatte, det fungerer ikke godt nok dessverre. Det gjelder på andre områder og ikke bare informasjonssikkerhet. Så veldig ofte blir folk ansatt og egentlig kastet rett inn i ansvarsoppgavene istedenfor å ta den tiden man burde til å sette folk inn i systemer, sikkerhetsnivåer og løsninger rundt det." (Informant F1).

Et problem som ble uttrykt blant en av informantene var at det var valgfritt å gjennomføre kurs og at det ikke var en obligatorisk del av ansettelsesprosessen:

> "Har pakker man må ha når man blir ansatt, i forhold til KS læring som vi bruker og der ligger ikke personvern og informasjonssikkerhet, "for det er det jo mange som

> ikke trenger", men jeg regner med at det vil komme inn som en del av en obligatorisk ansettelse. Per nå er det ikke det." (Informant C1).

Selv om det var valgfritt å gjennomføre kurs, ønsket noen av informantene at det skulle vært obligatorisk: "Det burde vært obligatorisk. Du skriver under en taushetsplikt, men du leser den ikke". Det blir også nevnt at informasjonssikkerhet er et så stort område og at kommunene fra før har mange fokusområder, noe som også har hindret dem i dette arbeidet: "Har ikke helt bestemt hvordan det skal gjøres, men noe må gjøres. Vi har to læringsportaler, men det er jo veldig mange fokus i en kommune, og informasjonssikkerhet er et veldig stort område." (Informant C1). I tillegg blir det å sette i gang med opplæringsinitiativer sett på som overveldende og det var vanskelig å vite hvor man skulle begynne:

> "Vi har ikke god nok systematikk for det, men jeg sier aldri nei, og er pådriver for at vi skal ta noen runder med alle enhetene, og da ønsker jeg egentlig med alle ansatte. Og vi har det på ledermøter innimellom, men vi er ikke systematiske nok, det er vi ikke. Og det er så stort det man skal ha fokus på, hvor skal man begynne?" (Informant G1).

Det kom også frem at opplæring var en viktig, men underkommunisert oppgave:

> "Opplæring og sikkerhetskultur, det er en underkommunisert og viktig oppgave. Fordi dette er noe som ikke har noe som helst verdi visst ikke man har folka med seg og det er forankret og forstått, og det er det et ønske om. Det er jo da man får effekt." (Informant A2).

Vi analyserte at ressurser var med på å bremse arbeidet med opplæring og sikkerhetskultur, særlig når det gjaldt å få innpass og oppmerksomhet hos de ulike virksomhetene i kommunen. Innenfor helse og velferd, samt oppvekst er det knapphet på tid, noe som har gjort det vanskelig å få innpass hos disse virksomhetene:

> "I deler av kommunen er man ganske presset på tid, både i helse og velferdssiden og oppvekstsiden, så kampen om tid er veldig hard. Så jeg har jo invitert meg ut til ulike virksomheter, "kan jeg få en halvtime på et personalmøte til å snakke om dette," og særlig på skolene har det vært veldig vanskelig å komme inn. Mengden med ting som de skal igjennom på et år, er mye, og da blir det opp til rektor å vurdere hvor viktig det er. Og sånn burde det egentlig ikke være tenker jeg." (Informant A1).

I en av kommunene ble det å dele og utveksle erfaringer med andre sett på som viktig og noe som bør gjøres for å bygge kompetanse:

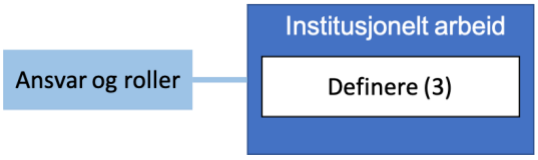
> "Jeg har jobbet mye i det private, ser at mange kommuner sitter hver for seg, det med å utveksle erfaring i større grad tror jeg er veldig viktig. For det gjøres jo noe godt arbeid både her og der, og vi er jo en ny kommune og prosessen vil foregå i mange år, men er mange som jobber smart, og det å kunne vite om hverandre tror jeg er viktig." (Informant H1).

I neste delkapittel presenteres resultatene fra analysen som omfavner ansvar og roller, hvilket er en forutsetning for god ISS.

7.2.4 Ansvar og roller

Å delegere tydelige ansvar og roller er en viktig del av arbeidet med ISS. Et ISS-dokument skal ha oversikt over ansvar og roller slik at dette kommer tydelig frem i organisasjonen. I rapporten fra Digitaliseringsdirektoratet (2020) fremkommer det at små og mellomstore kommuner trenger en veiledning til å beskrive roller og ansvar for støttefunksjoner på informasjonssikkerhet (s.14). Deres anbefaling var derfor: "Viktigheten av å beskrive roller og ansvar for informasjonssikkerhetsarbeidet bør tydeliggjøres for små og mellomstore kommuner". (Digitaliseringsdirektoratet, 2020, s. 23).

Arbeidet med å definere ansvar og roller kan henføres til institusjonelt arbeid, **definere,** hvor aktivitetene går ut på å lage systemer for regler, prosedyrer og status. Figur 11 viser oversikten over institusjonelt arbeid som ble identifisert under ansvar og roller.



Figur 11: Data kategorisert som institusjonelt arbeid under ansvar og roller

Flere av informantene uttalte at de hadde utarbeidet et overordnet styringsdokument hvor ansvar og roller var definert:

"Det er utarbeidet et overordnet styringsdokument, for informasjonssikkerhet og personvern, og der står sikkerhetsrollen definert da. Går mye på strategi og de ulike elementer som vi synes er viktig i forhold til arbeidet med informasjonssikkerhet, de ulike rollene da." (Informant C2). "Det jobber vi veldig mye med et sånt styringsdokument som sier hvem som skal gjøre hva av de forskjellige oppgavene i loven, hvilke roller som skal gjennomføre behandlingsprotokoll." (Informant E1).

> "Sånn som vi legger opp nå har jeg det øverste ansvaret for informasjonssikkerheten. Og så får, nå husker jeg ikke navn på roller, men jeg har fire kommunale sjefer som har sine ansvar, så de får sin rolle, så vil nok enhetsleder også få roller, og en systemansvarlig rolle i dette her. Så vi har satt opp et kart med en rekke roller, som noen får tildelt, og noen har fått tildelt allerede." (Informant J1).

Det var flere utfordringer som ble identifisert i forhold til komponenten ansvar og roller. Blant annet fører begrensede ressurser hos kommunene til at rollen som informasjonssikkerhetsansvarlige også fylles av mange andre ansvar og roller. I tilfeller kan dette være økonomiarbeider, beredskapskoordinatorer eller liknende som tar på seg ansvaret, hvilket gjør at arbeidet med informasjonssikkerhet kommer som et tilleggsansvar. I rapporten fra NorSIS (u.å) kommer det frem at det i flere kommuner er ansatte som får tildelt ansvar og roller som de egentlig ikke er egnet til:

> "Flere av de små kommunene som NorSIS har vært i dialog med har informasjonssikkerhetsansvarlige og behandlingsansvarlige, som i utgangspunktet har andre fagstillinger. Utfordringen med dette er at ansatte får dette ansvaret nærmest "dyttet" på seg. En økonomiansvarlig er for eksempel ikke automatisk dyktig til å foreta risikovurderinger og iverksette styringssystemer og prosesser knyttet til informasjonssikkerhet hvis en ikke får tilstrekkelig opplæring. Likeledes gjelder dette hendelseshåndtering. Dette er fagfelt som krever spesiell opplæring." (NorSIS, u.å, s.29).

Uklare roller og ansvar gjenspeiler seg også hos to av informantene:

> "Sikkerhetsrollen er jeg veldig fersk på, jeg jobber også, og er litt støtte innenfor beredskap, så jeg jobber veldig mye med koronarelaterte oppgaver. Jeg hadde jo ingen kompetanse innenfor sikkerhetsarbeid, informasjonssikkerhetsarbeid, og har jo heller ikke fått særlig tid til å bygge noe kompetanse i den perioden som er nå. Så jeg føler jeg har et hull der, men det er jo et spennende og viktig tema, men jeg har behov for mer kompetanse." (Informant C2).

> "I utgangspunktet er jeg beredskapskoordinator, 50% beredskapsarbeider og jobber med kvalitetssystemet, og rollen om å være personvernombud, men ikke stillingsprosent definert knyttet til det. Har et lite konfliktområde i og med at jeg skal være et ombud, samtidig utøvende rolle i kvalitetssystemet. Har i tillegg et kvalitetsprosjekt som går mye på internkontroll som vi skal prøve å bygge opp internt her på huset." (Informant F1).

Videre uttrykte flere av informantene at det var vanskelig å forstå hvem som hadde ansvar og roller i arbeidet med ISS, og at dette ikke kom tydelig frem:

> "Det som er utfordringen er hvem som er beslutningstaker på ulike områder, sånn som for eksempel sikkerhetsrutiner […]. Og så skal det være gjeldende for alle, det er mye sånt som er veldig uklart syntes jeg. Det kan hende det er klart, men at det ikke er gjort." (Informant C1).

"Det er ingen som har ansvar for å sikre, kan ikke peke på noen sikkerhetsansvarlig. Men IT-avdelingen har fokus på det, vi har VPN og tofaktor, har masse systemer, vi har personvernombud og vi har rutiner." (Informant I1). I tillegg er det mange mennesker å forholde seg til i en kommune og uten klare ansvar og roller var det vanskelig å se hvem som skal ta avgjørelser: "Det er veldig komplekst med informasjonssikkerhet. Er veldig mange hoder, ofte er utfordringen, hvem tar avgjørelser?" (Informant C1).

Videre bygde noen av ansvarsrollene seg på antakelser av at andre hadde ansvaret: "Jeg opplever jo ofte at folk antar ting, ja, men har ikke de ansvar for det? Nei de har faktisk ikke det. Hvis det går galt, så er det jo han sin skyld. Så det er det mye av." (Informant A2). Rollene som systemeier og systemansvarlig, som er ansvarlige for de systemene eller appene som blir kjøpt inn, samt sikkerheten for disse, var i noen tilfeller ikke definert godt nok: "Det ligger mye i systemeierrollen og systemansvarligrollene, men der ligger det også mye mer og det er roller som er litt […]. De er ikke tydelige nok i organisasjonen." (Informant G1). I en av kommunene var det én person som hadde ansvaret for å utforme ISS og så på dette som vanskelig da informanten i tillegg jobbet med flere andre oppgaver:

> "Jeg mener at vi hvert fall skal bistå med mer enn en person i det arbeidet, for det er en del av det jeg jobber med. Hvis jeg hadde fått jobbet bare med det, så kunne jeg gjerne gjort det selv, men det tar en ørliten del av alt jeg jobber med i det daglige. Det er vanskelig å finne nok ressurser til å jobbe godt alene med dette i en middels stor kommune." (Informant G1).

Press på ressurser og at man hadde mange områder å fylle, var betegnet som en av de store utfordringene i arbeidet med utformingen av ISS: "Det er sånn at det er så press på ressurser, og mange som jobber med daglig driftsoppgaver." (Informant G1). I en annen kommune var det en av informantene som mente det var vanskelig å jobbe med ISS alene, og at flere mennesker som samarbeidet var en forutsetning for å få til et godt arbeid:

> “Var en i kommunedirektørens stab som hadde denne rollen, men det er ikke veldig enkelt å jobbe alene med dette. Så når jeg startet med dette så sa jeg at jeg skulle ta på meg denne, men med forutsetning at jeg fikk plukke med meg folk fra områdene. For det er da man får jobbet godt med det” (Informant H1).

I neste kapittel diskuteres resultatene fra analysen i sammenheng med relevant litteratur og forskning.

8. Diskusjon

Før vi begynner å diskutere utfordringer og mulige løsninger innleder vi med å diskutere hvorfor noen typer institusjonelt arbeid ikke ble identifisert.

I resultater og analyse var det flere typer institusjonelt arbeid vi ikke identifiserte. Blant annet hadde vi ingen kildedata fra informantene som passet med *forhindre institusjoner* og dette stemmer godt overens med Lawrence & Suddaby (2006) om at det sjeldent blir identifisert denne typen institusjonelt arbeid. Det ble heller ikke funnet institusjonelt arbeid i form av *opptjening, mimikk, avskrekking, valorisering og demonisering eller mytologisering*. Det kan diskuteres om dette er som følge av kildedataen og at et annerledes datagrunnlag kunne ført til at man ville identifisert flere eller andre typer institusjonelt arbeid enn det som fremgår i denne studien. På en annen side kan det diskuteres om disse typene institusjonelt arbeid ikke er vanlig å praktisere når man arbeider med ISS.

Videre i dette kapittelet diskuterer vi empirien fra resultater og analyse knyttet opp mot litteratur og teori. Kapittelet er delt i to deler, i første del diskuteres utfordringer med ISS og årsakene til utfordringene. I del to diskuteres forslag til ulike løsninger på utfordringene slik at man kan oppnå et bedre og mer vellykket arbeid med ISS.

8.1 Utfordringer med ISS i norske kommuner

I dette avsnittet diskuteres de ulike utfordringene og årsakene til disse som vi identifiserte i empirien i resultatkapittelet og diskuterer dette opp mot teori og litteratur. Institusjonell logikk er med på å forklare årsaker til utfordringene under de ulike ISS-komponentene, men vi ønsket også å inkludere et eget avsnitt om logikk da vi mener det er viktig å diskutere hvilke utfordringer som kan oppstå når ulike logikker møtes.

8.1.1 Institusjonell logikk

I analysedelen identifiserte vi to logikker som utmerket seg fra dataene våre; byråkrati- og profesjonslogikk. Markedslogikk/NPM ble ikke identifisert, og det kan diskuteres om denne logikken i det hele tatt brukes i sammenheng med ISS. Som Thornton et al., (2012) skrev, kan individer skifte mellom ulike logikker i forhold til det arbeidet de gjør eller situasjonen de befinner seg i. Arbeidet med ISS er i stor grad basert på kontroll, overordnet styring og prosedyrer (AlGhamdi et al., 2020), hvilket representerer byråkratilogikk.
Flere informanter var enig i at det var nødvendig med en byråkratisk styring for å få til et godt arbeid med ISS. På den andre siden mente noen at dette kunne være negativt ved at kommunene fikk mer avstand til arbeidet med ISS. Det er sterke indikasjoner på at ulike fagbakgrunner og profesjoner fører med seg ulik logikk som kan være med på å forklare hvorfor det ofte oppstår gnisninger og utfordringer opp mot enkelte virksomheter slik som skole og oppvekst i arbeidet med ISS. Dette stemmer godt overens med litteraturen som beskriver at institusjonell logikk kan være med på å forklare motstridende praksiser og oppfatninger i institusjoner (Wahid & Sein, 2013). I tillegg bekrefter det at daglige situasjoner og handlinger innad i kommuner er formet av ulike logikker (Fred, 2020).

Videre viser analysen at profesjonslogikk hos virksomhetsområdene innad i kommunene er med på å både forhindre og forenkle arbeidet. Dette kan relateres til institusjonell pluralisme, hvilket kan forklare bakgrunnen til utfordringene med å praktisere ISS mot ulike virksomheter i kommunen. Analysen viser tydelig at det ikke finnes noen dominerende

logikk og at flere logikker skaper spenninger slik det blir betegnet i litteraturen (Reay & Hinings, 2009). Byråkratilogikk og profesjonslogikk ser ut til å fungere bedre sammen i helse og omsorg, enn hos skole og oppvekst. Spenningene mellom de ulike logikkene kan derfor forklare årsaker til utfordringene som oppstår i arbeidet med ISS, særlig mot enkelte virksomheter. Det kan diskuteres om profesjonslogikk innen helse og omsorg er enklere å arbeide med når det gjelder ISS, og at denne logikken fungerer godt med prinsippene som ligger bak ISS, slik som rutiner og prosedyrer, avvikskultur, personvern og informasjonssikkerhetsstyring. Motsatt gjelder for skole og oppvekst som virker å ha mindre fokus på informasjonssikkerhet, og en kultur som bygger mer på myke verdier, mangfold, å være kreativ og velge sine egne digitale verktøy i yrkesutøvelsen. Det kan diskuteres om bygging av en sikkerhetskultur bør starte allerede i utdannelsen til lærere, slik at de blir programmert til å tenke på informasjonssikkerhet på samme måte som helsearbeidere.

8.1.2 Revisjoner og kontroll

Å revidere og evaluere virksomhetens mål og sikkerhetsmekanismer er en viktig del av arbeidet med ISS og gjør at man kan etterleve, kontrollere og optimalisere ISS (AlGhamdi et al., 2020; Williams et al., 2013). Revisjon er en viktig komponent for å evaluere hvilket ISS-modenhetsnivå man ligger på (Yaokumah, 2014), slik at man proaktivt kan identifisere utfordringer som må tas hånd om (Carcary et al., 2016). I tillegg er revisjon og kontroll en viktig komponent i Digitaliseringsdirektoratet sin veiledning om ISS (Digdir, u.å-f). I rapporten fra Digitaliseringsdirektoratet (2020) kommer det frem at under 50% av små og mellomstore kommuner evaluerer, forbedrer eller fornyer styringssystemet. Funn blant informantene bekrefter dette, og det kan diskuteres om press på ressurser og vanskeligheter med å kontrollere avvik, er en forklaring på denne utfordringen. Som presentert i resultater og analyse er "politiarbeid" en del av revisjoner og kontroll og var den typen institusjonelt arbeid som var mest vanlig. Når denne typen institusjonelt arbeid ikke fungerer godt nok, som følge av press på ressurser og manglende rutiner, kan det føre til utfordringer med å endre institusjonen og logikkene slik at de støtter arbeidet med ISS.

Det ble bekreftet at flere informanter ønsket å gjennomføre revisjoner og kontroll, men at knapphet på ressurser førte til at dette ikke ble prioritert. Det kom frem at kommunedirektøren ikke interesserte seg nok for det og hverdagen ikke strekte til, hvilket førte til at man heller prioriterte andre områder. Dette bekreftes også i litteraturen, der det blir betegnet som utfordrende å sette av ressurser til noe som ikke har skjedd og være proaktiv når det kommer til informasjonssikkerhet (Carcary, 2016).

Avvik ble i en kommune brukt til å kontrollere og revidere for å se hvilke områder og virksomheter de trengte å jobbe mer mot når det gjaldt informasjonssikkerhet. Å holde oversikt over risiko og trusler er viktig for suksessfull ISS slik at man raskt kan respondere på nye trusler, samt kontinuerlig optimalisere ISS (AlGhamdi et al., 2020). Selv om noen informanter klarte å bruke avvik til å kontrollere og revidere, opplevde flere informanter utfordringer. Blant disse ble det nevnt utfordringer med at det var en oppfatning om at de som kontrollerte avvik virket "skumle" og man risikerte at avvikene ikke ble meldt. Det var også flere informanter som uttrykte at ansatte så på avvik som noe negativt, at det handlet om sladring og var et negativt ladet ord. Det var derfor flere informanter som snakket om at det var viktig med en kulturendring slik at avvik var assosiert med noe positivt og forbedringsmuligheter.

Selv om litteraturen ser på privat sektor og ikke snakker om avvik i direkte forstand, kan det diskuteres om avvik også er en form for risikostyring og kontrollmekanisme, ettersom det legger til rette for rapportering og respons på utfordringer med sikkerheten. Yaokumah (2014) skrev at risikostyring er oppnådd når man har sikret at risikoevalueringer og skadebegrensninger er integrert i den daglige driften, som fører til rask rapportering og respons på utfordringer med sikkerheten. Dette gjør at man kan sikre IT-eiendeler, rask gjenoppretting etter angrep, forretningskontinuitet, samt minimere risiko og redusere uheldige innvirkninger på informasjonseiendeler (Yaokumah, 2014). Ettersom vi ser på avvik som en viktig del av risikostyring, revisjon og kontroll, kan det diskuteres om utfordringer med å registrere avvik bør adresseres omgående hos de ulike kommunene som ikke klarer å ta i bruk avvik som en del av styring og kontroll.

8.1.3 Eierskap

Eierskap var et viktig funn i dataanalysen og handler om at man skal inkludere flere nivåer og virksomheter i kommunene i arbeidet med å utforme ISS, for at alle skal få et eierskap til ISS. Forskningen var delt når det kom til hvordan dette burde gjøres og noen fremmet en desentralisert tilnærming, der man involverte aktører på tvers av alle nivåer (Rannenberg et al., 2010; Tan et al., 2017). På en annen side fremmet noen en sentralisert tilnærming, der toppledelsen kommuniserer ovenfra og ned (Fazlida & Said, 2015; Nærø, 2020). Vi la merke til at rapporten fra Digitaliseringsdirektoratet (2020) ikke spesifiserte noe om eierskap eller anbefalinger relatert til desentralisert vs. sentralisert styring. Det kan diskuteres om det er en utfordring at dette ikke har blitt satt høyt nok på agendaen blant offentlig forvaltning, og er en underkommunisert og viktig del av ISS. Ressurser var igjen en utfordring, og når press fra direktoratene baserte seg på bør og ikke skal ble det ikke bevilget ressurser til det man bør, men bare til det man skal. Derfor var man avhengig av at kommunedirektøren og kommuneledelsen var supersupporter for informasjonssikkerhet og på den måten tok man et eierskap til arbeidet med ISS.

Sentralisert og desentralisert tilnærming er en viktig del som kan diskuteres om er en utfordring i kommunene. I en kommune ønsket de å bruke en ovenfra og ned tilnærming, der ledelsen jobbet sentralt med å utarbeide ISS. På en annen side påpekte de samtidig at en utfordring kunne være at ikke alle ville få et ordentlig eierskap til arbeidet med ISS. En av informantene fortalte at sentralisering kan være positivt for små kommuner da de har begrensede ressurser. Denne typen styring viser eksempler på byråkratilogikk og det kan diskuteres om denne logikken hindrer virksomhetene i å ta eierskap til ISS-arbeidet. I tillegg identifiserte vi **"**etablere normative nettverk" som viktig institusjonelt arbeid, som støttet eierskap ved å etablere arbeid på tvers, og sørge for eierskap på alle nivåer. Det kan diskuteres hvorvidt det kan oppstå utfordringer med at byråkratilogikk som kjennetegnes av en overordnet og sentral styring, ikke støtter denne typen institusjonelt arbeid. I litteraturen var det delte meninger om man bør ha en sentralisert eller en desentralisert tilnærming, noe som også gjenspeilet seg blant informantene. Det kan diskuteres om det er en utfordring at det er såpass delte meninger rundt dette og at det burde komme mer forskning på hva som er den beste måten å styre på innenfor offentlige organisasjoner. En av informantene uttrykte at kommunedirektører i små kommuner ønsket at IKT-samarbeidet tok alt ansvaret med ISS, og styrte dette ovenfra og ned til kommunene. Med dette oppstår det spørsmål om man møter på utfordringer med mindre eierskap, samt en falsk trygghet om at "informasjonssikkerhet tar noen andre seg av".

8.1.4 Opplæring og sikkerhetskultur

En viktig del ISS er med på å understøtte er det å bygge en god informasjonssikkerhetskultur (Sørgård, 2013; Veiga & Eloff, 2007) hvor sikkerhet sitter fremst hos alle nivåer i virksomheten (AlGhamdi et al., 2020). I rapporten fra Digitaliseringsdirektoratet (2020) kommer det frem at kommuner ikke arbeider godt nok med kompetanseheving og sikkerhetskultur, noe som også gjenspeilet seg blant flere av informantene. Systematikk rundt dette arbeidet og begrenset kompetanse blant ledere var også et problem som oppsto ifølge noen informanter. I de litt større kommunene, var det mange nyansatte hvert år, noe som gjorde det vanskelig å ha gode rutiner og forvalte arbeidet med opplæring og sikkerhetskultur. Mellom de ulike kommunene var det variasjoner i forhold til å kontrollere om ansatte hadde gjennomført opplæring, der noen baserte seg på tillitt, mens andre brukte statistikk. Flere av informantene uttrykte at det var først etter hendelser som i Østre Toten at man fikk fokus på viktigheten med dette arbeidet.

Institusjonelt arbeid i form av "utdanning" var ikke alltid lett å gjennomføre, da en utfordring var at folk bare ble kastet ut i de oppgavene de hadde, istedenfor å sette av ressurser og tid til opplæring. En annen utfordring var at det var valgfritt å gjennomføre kurs og man kan derfor ikke sikre at alle gjennomfører kursene. Det kan diskuteres om dette svekker institusjonelt arbeid som **"**utdanning", da man ikke har noen garanti for at opplæring blir gjennomført. En annen viktig utfordring kan forklares av at når ansatte har mange andre fokusområder i kommunen som de også trenger opplæring i, kan det føre til at informasjonssikkerhet nedprioriteres. Ressurser var en faktor som skapte utfordringer for opplæring og sikkerhetskultur da virksomheter som helse og velferd, samt oppvekst ikke hadde tid til å prioritere opplæring. Dette bekrefter tidligere funn (NorSIS, u.å), om at ressurser er en barriere når det kommer til arbeidet med informasjonssikkerhet.

8.1.5 Ansvar og roller

ISS bidrar med rammeverk for å imøtekomme krav, håndtere risiko i virksomheten og etablerer klare roller og ansvarsområder (Moulton & Coles, 2003), noe som er en viktig faktor for god informasjonssikkerhet (Gashgari et al., 2017; Mishra, 2015). Det er derfor sett på som essensielt for ISS å definere tydelige ansvarsområder og roller. Når det kommer til institusjonelt arbeid handlet dette i hovedsak om "definere"**,** ettersom arbeidet med å delegere ansvar og roller handler om å lage oversikt og prosedyre for hvem som gjør hva. I noen kommuner var ikke denne typen institusjonelt arbeid utarbeidet tydelig nok og den enkeltes ansvar var i liten grad definert. Dette utpekte seg som en utfordring i enkelte kommuner, hvilket kan være med på å forklare hvorfor deres ISS ikke er innarbeidet godt nok og at praksis ikke blir gjennomført i henhold til retningslinjer. I et ISS-modenhetsperspektiv er uklare ansvarsområder og roller definert som nivå 1 og 2 (Yaokumah, 2014), hvilket tilsier at ISS er på et nivå hvor det er "ikke eksisterende" eller i beste fall "innledende".

Mange av de ansatte i kommunene har flere roller å utfylle, og informasjonssikkerhetsrollen kommer gjerne som en tilleggsrolle. I rapporten fra NorSIS (u.å) kom det frem at en utfordring var at ansatte fra andre fagstillinger får tildelt ansvar og roller som informasjonssikkerhetsansvarlig og behandlingsansvarlig. Dette gjenspeilet seg også hos to av informantene, hvor de enten hadde lite kompetanse innenfor informasjonssikkerhetsarbeid, eller ikke definert stillingsprosent til dette arbeidet. I tillegg var informantene presset på tid og ressurser, samtidig som arbeidet med ISS bare var en liten del av det daglige arbeidet.

Støtte fra toppledelsen er viktig for å imøtekomme ISS-initiativer (Gashgari et al., 2017), men dette ble sett på som en utfordring hos flere av informantene. Videre er mangel på støtte fra toppledelsen en barriere for adopsjon av ISS-rammeverk og standarder (Gillies, 2011). Flere av informantene bekreftet dette, og mente at det var essensielt at kommunedirektøren stod i spissen som en supporter for arbeidet med ISS. En av informantene uttrykte at man ikke fikk gjennomført ISS så lenge kommunedirektøren ikke var interessert. I tillegg mente en informant at toppledelsen ikke alltid hadde informasjonssikkerhet øverst på agendaen, noe som kunne gjøre det vanskelig å arbeide med ISS. Basert på dette kan manglende støtte fra toppledelsen være med på å forklare hvorfor det i flere av kommunene var vanskelig å jobbe med ISS og kommunisere dette arbeidet til alle nivåer og virksomheter i kommunen.

8.2 Mulige løsninger på utfordringene med ISS

Digitaliseringsdirektoratet pekte på at de ønsket å finne årsaker til hvorfor de mindre og mellomstore kommunene hadde så store utfordringer med ISS. Flesteparten av kommunene vi snakket med hadde problemer med å praktisere ISS på en god måte og bekrefter dermed funnene i rapporten fra Digitaliseringsdirektoratet (Digdir, 2020). Vi ønsker derfor å diskutere, på bakgrunn av litteratur og forskning, ulike forslag til løsninger på noen av disse utfordringene.

8.2.1 Institusjonell logikk

Når det kommer til utfordringene relatert til de institusjonelle logikkene, kan en løsning være å etablere flere samarbeidsaktiviteter, nettverk, samt skape en dominanskultur og produksjon eller vedlikehold av institusjonelle regler (Reay & Hinings, 2009). Samarbeidet kan videre være med på å håndtere de ulike interessene som til slutt skaper endringer i de institusjonelle logikkene. Dette krever at man etterlater seg sin gamle logikk og identitet, og utvikler en ny i samarbeidet (Reay & Hinings, 2009). I gjennomgangen av resultater og analysen viste vi til en ny logikk som vi valgte å kalle ISS-logikk. Denne logikken har symbolske og materialistiske verdier som samarbeid på tvers, deling av informasjon, positiv assosiasjon til avvik, og kontroll og revisjon. Det kan diskuteres om denne logikken har bidratt til hvorfor en av kommunene sitt arbeid med ISS fungerer så bra. Samarbeid på tvers, som vi definerte som en av verdiene bak ISS-logikken, er ifølge Poore (2005) en viktig komponent for å oppnå god styring. I tillegg brukte en av kommunene et nettverkssamarbeid aktivt i arbeidet med ISS og de rapporterte et høyt antall avvik som følge av dette. Dette kan være med på å bekrefte antagelsene om at nettverkssamarbeid har skapt en ny identitet og logikk på tvers. Det å ha en positiv assosiasjon til avvik blir nevnt av flere av informantene som viktig. Dette er eksempler på verdier som ligger bak ISS-logikken, og denne logikken ses på som viktig i sammenheng med verdier som fremmer arbeidet med ISS. Det kan derfor diskuteres om ISS-logikken har vært nyttig i å få med alle ansatte og virksomheter i kommunen til å støtte arbeidet med ISS og øke antall avvik.

8.2.2 Revisjoner og kontroll

I rapporten fra Digitaliseringsdirektoratet (2020) kommer det frem at under 50% av kommunene reviderte og forbedret styringssystemet for informasjonssikkerhet som en del av ISS-arbeidet. Dette samsvarer ikke med funnene i litteraturgjennomgangen ettersom det er

viktig å ha oversikt over trusler og risiko til enhver tid og gjøre regelmessige trusselvurderinger (AlGhamdi et al., 2020; Gashgari et al., 2017). Videre manglet flere av informantene den kontrollerende delen av ISS. Det bør etableres enkle og fleksible kontrollmekanismer (Mishra, 2015), samt en oversikt over trusler og risiko til enhver tid for å aktivt kunne respondere på nye trusler, dette er viktig for suksessfull ISS (AlGhamdi et al., 2020).

Institusjonelt arbeid slik som "politiarbeid", er med på å støtte arbeidet med revisjoner og kontroll, både i form av sikkerhetsrevisjoner ute hos virksomhetene og kontroll av avvik. Denne formen for institusjonelt arbeid var viktig for flere av informantene og førte til, som en informant uttrykte, får ringen slutta og man får kontrollert om virksomhetene gjør det de skal. I de tilfellene "politiarbeid" ikke fungerte som institusjonelt arbeid handlet det mye om hvilke assosiasjoner man hadde til avvik. En kommune brukte rapporter, revisjoner og kontroll for å ha oversikt over virksomhetenes arbeid med informasjonssikkerhet og hvor det var forbedringsmuligheter. Det at virksomhetene gjør en bevisst handling var i tillegg med på å bevisstgjøre avviksmeldinger. Vi mener denne kommunen viser et godt eksempel på hvordan man kan arbeide med ISS, hvor de både har en gjennomførende og en kontrollerende del, slik at man kan få oversikt over tilstanden og se rom for forbedringer. Det kan diskuteres om dette også er en form for overvåking av ansatte som Veiga (2007/2004) anbefalte, slik at man kan sikre etterlevelse av sikkerhetskrav. AlGhamdi (2020) påpekte også viktigheten med å måle, utarbeide rapporter og evaluere slik at man får en tilstandsrapport over ISS-arbeidet og en oversikt over hvor langt man har kommet.

Avvik er en viktig indikator og henger sammen med revisjon og kontroll ettersom man kan kontrollere hvor mange avvik som blir rapportert hos de ulike virksomhetene. Med dette kan man sikre etterlevelse ved å få en oversikt over hvor langt man har kommet i arbeidet med ISS (AlGhamdi, 2020). I en kommune, der informantene rapporterte at det ble meldt mye avvik, spilte nettverket, hvilket vi definerer som "etablere normative nettverk" under institusjonelt arbeid, en viktig rolle. I dette nettverket diskuterte de utfordringer og delte kunnskap og erfaringer på tvers, noe som ble sett på som en av grunnene til deres suksess med ISS. Slayton (2021) skrev at det er nyttig å ta i bruk nettverk for å involvere alle aktører i arbeidet med ISS og skape en felles forståelse, dette kunne også forbedre arbeidet med risikostyring. I tillegg innarbeidet en kommune tanken om at avvik var noe som ble applaudert, som vi plasserte under "teoretisering" og "endring av normative assosiasjoner". Igjen blir det brukt en kombinasjon av ulike typer institusjonelt arbeid. Det kan diskuteres om denne tilnærmingen til ISS vil kunne fungere for andre kommuner også, og at blant annet bruk av nettverk som institusjonelt arbeid støtter ISS på en god måte. I tillegg ligger det i arbeidet å endre tankegangen hos de virksomhetene de reviderte og kontrollerte. Innen institusjonelt arbeid kan dette defineres som "etablere identiteter" ettersom mye handler om å endre tankegangen til mennesker slik at de støtter institusjonen og arbeidet med revisjoner og kontroll.

8.2.3 Eierskap

Når det kommer til eierskap og sentralisert vs. desentralisert styring var det delte meninger om dette både i litteraturen og blant informantene. Basert på en av kommunene ser man at en desentralisert tilnærming har vært nøkkelen til deres suksess med ISS, og var med på å sikre at alle nivåer og virksomheter som ble med i prosessen, fikk et eierskap og økende bevissthet rundt informasjonssikkerhet. For å kunne oppnå godt eierskap krever det at prosessene er

utviklet og på plass (Maynard et al., 2018; Rannenberg et al., 2010). På bakgrunn av dette kan det derfor diskuteres om en desentralisert styring fungerer bra for små og mellomstore kommuner, da den ene kommunen var den vi analyserte å ha kommet lengst i arbeidet med ISS. Eierskap er også viktig når det kommer til å utforme retningslinjer og å involvere ansatte i å utforme disse, slik at man kan unngå at retningslinjene blir avvist eller ikke blir fulgt (Fazlida & Said, 2015). Noen av kommunene ønsket å involvere flere i denne utformingen og dette kan vi diskutere om er en viktig faktor for å sikre at retningslinjer blir implementert og fulgt.

En av kommunene delte skjerm med oss og viste at de hadde kartlagt en stor andel av prosessene i kommunen med flytdiagram, hvor alle ansvarsområder og roller var tydelig definert. Prosessene for ISS var også på plass og illustrerte hvem som var involvert i dette arbeidet på alle nivåer. Det kan diskuteres hvorvidt kommunene bør kartlegge prosessene slik det ble gjort i denne ene kommunen, kombinert med en desentralisert tilnærming til styring. På denne måten kan man sikre eierskap blant de ulike enhetene og virksomhetene for å sikre en mer vellykket ISS og kjennskap til retningslinjer. Fra et ISS-modenhetsperspektiv er definerte prosesser nivå 4, men ettersom den ene kommunen også har klare roller og ansvarsområder samsvarer det med nivå 5 (Yaokumah, 2014), og vi kan anta at kommunen ligger et sted mellom modenhetsnivå 4 og 5. Ettersom litteraturen ser på eierskap som et viktig område innen ISS, kan det diskuteres om det bør komme høyere opp på agendaen for offentlig forvaltning og hos kommuner, da desentralisert og sentralisert styring ikke blir spesifisert i rapporten fra Digitaliseringsdirektoratet (Digitaliseringsdirektoratet, 2020).

Når det kom til institusjonelt arbeid var "etablere normative nettverk" det mest prominent funnet som støttet eierskap. For en av kommunen var et nettverk som samlet virksomhetene gjennom møter og seminarer med på å skape innsikt i problemstillingene som virksomhetene opplevde i forhold til informasjonssikkerhetsarbeidet. Dette var også støttet av arbeid på tvers, og det kan diskuteres om byråkratilogikk ikke vil passe inn i dette arbeidet. En av informantene hadde flere tydelig trekk som samsvarte med de symbolske og materialistiske elementene i ISS-logikken. Denne logikken tolker vi at passer godt i arbeidet med å **"**etablere normative nettverk", da en av kjerneverdiene er samarbeid på tvers, og at det fungert i såpass stor grad i denne kommunen.

8.2.4 Opplæring og sikkerhetskultur

Ved å ta i bruk et ISS-rammeverk oppnår man bedre oversikt over opplæringsinitiativer og sikkerhetskulturen i virksomheten (Veiga & Eloff, 2007). Det er viktig å kontinuerlig arbeide med opplæring og sikkerhetskultur i en virksomhet for vellykket ISS (Gashgari et al., 2017). En måte å jobbe med sikkerhetskultur på gjennom institusjonelt arbeid, er å kombinere flere ulike typer institusjonelt arbeid for å skape kulturendring. Kultur står sterkt i institusjonell teori og som i definisjonen til Thornton et al., (2012), består logikker blant annet av kulturelle verdier. Institusjonelt arbeid er med på å endre logikkene og derfor også de kulturelle verdiene. Det var derfor interessant å identifisere hvilke type institusjonelt arbeid som støtter arbeidet med sikkerhetskultur og opplæring. Typen institusjonelt arbeid vi identifiserte flest ganger her var "utdanning", og revisjonen av Sandnes kommune som vi fortolker som en best praksis kommune, viser i tillegg til bruken av "normative nettverk" for å dele erfaringer og lære av hverandre. Reay & Hinnings (2009) bekrefter at samarbeidsaktiviteter kan føre til endring i de institusjonelle logikkene og vi mener at et nettverksamarbeid er et eksempel på en slik aktivitet hvor man bygger sikkerhetskultur og bevissthet rundt informasjonssikkerhet.

Videre hadde Sandnes kommune jevnlig faglige forum og samarbeid med virksomhetene for å opprettholde og øke kunnskapen, samt dele denne med hele organisasjonen. Innenfor institusjonelt arbeid kan dette relateres til både "utdanning", "innbaking og rutine", samt "etablere normative nettverk". På bakgrunn av dette mener vi at arbeidet med opplæring og sikkerhetskultur handler om å konstant innarbeide og fremme en sikkerhetskultur gjennom godt samarbeid og jevnlige møter med virksomhetene, og ikke kun sette sin lit til "utdanning" og opplæringsverktøy som KS læring. Et godt arbeid med sikkerhetskultur og opplæring vil øke ISS-modenheten, og sikkerhetsbevissthetsprogrammer ligger på nivå 4 "definerte prosesser" (Yaokumah, 2014).

På bakgrunn av det informantene uttrykte om opplæring og sikkerhetskultur kan man se at institusjonelt arbeid i hovedsak har handlet om å gi opplæring som kan betegnes som "utdanning" og revidere og kontrollere gjennom "politiarbeid". Når det kommer til "utdanning" var det bekreftet blant våre informanter som en viktig faktor som drev arbeidet med opplæring og sikkerhetskultur fremover. Denne typen arbeid ble gjort best med å tenke aktiv læring, jobbe med opplæring og sikkerhetskultur over tid, gjennomføre veiledninger og kurs, samt sikre at ansatte gjennomfører kursene med gode rutiner.

For en av kommunene var "politiarbeid" en viktig komponent for å bygge sikkerhetskultur og kontrollere arbeidet med informasjonssikkerhet hos virksomhetene. De så at det har vært en endring der virksomhetene som i starten syntes det var skummelt å bli revidert, og hvor bruk av ord som "forbedringsmuligheter" var med på å skape en holdningsendring blant lederne hos virksomhetene, nå blir sett på som mer positiv. Dette viser eksempel på at institusjonelt arbeid kan bidra til å endre logikk til å bedre støtte det arbeidet man utøver. En kommune hadde opplevd tilsvarende, og klarte å endre det negativt ladde ordet "avvik" til noe positivt, og formidlet dette i hele kommunen slik at de ulike virksomhetene skulle se på dette som et forbedringsverktøy og ikke noe "farlig". Basert på Lawrence (2006) blir dette referert til som den første delen av institusjonelt arbeid, "skape institusjoner", og er med på å skape bevissthet, ferdigheter og refleksivitet hos de ulike virksomhetene. Selv om dette arbeidet fungerte hos en kommune, var det andre som uttrykte at dette arbeidet var vanskelig å gjennomføre og følge opp ordentlig. Utfra datamaterialet kan det tyde på at kommuner som har personer som jobber fulltid med ISS, har en større mulighet for å oppnå høyere modenhet, i tillegg til at det er enklere å formidle budskapet om sikkerhetskultur til alle virksomhetene i kommunen.

Ressurser var en utfordring som ble nevnt å hindre arbeidet med opplæring og sikkerhetskultur. Basert på intervjuene var det flere av informantene som hadde andre ansvarsområder i tillegg til å jobbe med ISS. Dette gjorde at de ikke hadde ressurser og tid til å sørge for et godt systematisk arbeid med opplæring og sikkerhetskultur. I tillegg hadde en av informantene opplevd at virksomheter som skole og helse ikke ønsket å prioritere informasjonssikkerhet og ønsket innpass av informasjonssikkerhetsansvarlig på møter. Det kan derfor diskuteres om det i noen kommuner bør bevilges mer ressurser til dette området slik at man sikrer en høyere sikkerhetskultur, hvilket igjen kan øke ISS-modenheten. På denne måten kan man proaktivt imøtekomme fremtidige trusler og ivareta innbyggernes integritet.

8.2.5 Ansvar og roller

Under ansvar og roller bestod institusjonelt arbeid av å "definere", hvilket handler om å definere regler, retningslinjer og prosedyrer. En måte å gjøre dette på er å utarbeide et overordnet styringsdokument. Flere av kommunene jobbet med dette aktivt, men på en annen side var det hos noen kommuner uklare roller og ansvarsområder relatert til ISS-arbeidet. En løsning på dette kan være å ta i bruk et ISS-rammeverk slik som ISO27001 eller veilederen fra Digitaliseringsdirektoratet (Digdir, u.å-e) som en av kommunene hadde gjort. På den måten kan man også oppnå høyere ISS-modenhet (Veiga & Eloff, 2007) og klare ansvar og roller er en forutsetning for høyere modenhetsnivå (Yaokumah, 2013). Det er viktig å få frem at det å tildele klare ansvarsområder og definere tydelige roller er en viktig forutsetning for informasjonssikkerheten (Gashgari et al., 2017; Mishra, 2015).

Ettersom det blant flere informanter ble uttrykt at det ikke var klare ansvarsområder, indikerer det at toppledelsen ikke har vært god nok til å kommunisere hvem som har ansvar for hva. Først når man har sikret tilstrekkelig støtte fra toppledelsen kan man sette i gang arbeidet med ISS (Posthumus & von Solms, 2004). Toppledelsen skal være delaktig i å etablere overordnede mål, og retningslinjer bør brytes ned til det taktiske og operasjonelle nivået (von Solms et al., 2011). Med dette kan man sikre at retningslinjer og mål blir realisert hos alle nivåer fra øverst i kommunene, til virksomhetslederne og det operasjonelle. Toppledelsen bør delegere ansvar og eierskap til styring (von Solms & von Solms, 2004) ut i de ulike virksomhetene, så man har ansvarlige som er mer bevisste rundt informasjonssikkerhet og hvilke retningslinjer som gjelder. For å få til god ISS bør toppledelsen vise deres forpliktelse til arbeidet, støtte mål og misjon, samt informasjonssikkerhetsstrategien (Posthumus & von Solms, 2004; Whitman & Mattord, 2011). Det å ha egne dedikerte sikkerhetsroller viser seg også å være nyttig da vi har et inntrykk fra våre informanter at de som hadde definert denne rollen hadde større fokus på ISS.

Til slutt er ansvar og roller en kategori der ressurser er en utfordring. Det ble uttrykt blant informantene at de hadde begrensede ressurser og mange roller å fylle. Det virker derfor tydelig at det i noen av kommunene er utilstrekkelig med ressurser tildelt til arbeidet med ISS.

Så langt i dette kapittelet har vi diskutert mulige løsninger på noen av utfordringene som er adressert fra resultater og analyse. Neste delkapittel vil bestå av en beskrivelse av begrensningene i studien.

8.3 Begrensninger

Følgende begrensninger adresseres i studien; vi har valgt å avgrense utvalget til informanter som for det meste hadde lederroller sentralt i kommunen. Hvis vi hadde inkludert informanter fra operasjonelle nivåer og virksomhetsledere som ofte ble omtalt av informantene, ville vi fått et mer nyansert synspunkt. Utvalget av informanter gjenspeiler derfor kun et synspunkt og vi har hverken fått bekreftet eller avkrefte påstandene deres av andre. En annen begrensning kan relateres til at ISS er så komplekst og flere av komponentene flyter så inn i hverandre at det er vanskelig å holde dem atskilt. Det finnes derfor en risiko for gjentakelser av empiri og vi har prøvd til beste evne å se over dette. Videre er modenhetsnivåene kun basert på analysen av informantenes utsagn. En slik måling bør gjøres mer systematisk og nøyaktig, og kan defineres som en begrensning. På en annen side er dette ikke et mål med studien, men vi har hatt data til å kunne gi indikasjoner på hvor kommunene omtrent ligger i modenhet. Videre er det gitt en rik beskrivelse av kontekst og fenomen som gjør det mulig for at studien kan overføres til andre sammenhenger som et forsøk på å møte noen av begrensningene. Begrensninger som er relatert til valgt teori er adressert i teorikapittelet og begrensninger utover dette kan relateres til at de valgte teoriene kun gir en linse, men sådant et gyldig bilde, som bidro til dypere forklaringer, noe vi mener denne studien har illustrert.

9. Konklusjon

Enkeltcasestudien har vist at det er mulig å kombinere to viktig retninger innen institusjonell teori som analyseverktøy; institusjonell logikk og institusjonelt arbeid. Teorien i kombinasjon med metoden har gitt et nyansert bilde på utfordringer møtt av aktører involvert i arbeidet med ISS. Bruk av institusjonell logikk og institusjonelt arbeid har sammen bidratt til studiens forklaringskraft og en dypere og mer nyansert diskusjon. Studien er også blant den eneste i sitt slag, og bidrar med forskning på et underrepresentert område innen teorien, ISS i praksis og kombinasjonen av teori og praksis. Studien illustrerer hvordan individer bidrar til å forme institusjoner gjennom institusjonelt arbeid. I tillegg har vi diskutert forholdet mellom institusjonelt arbeid og logikker, hvor det kan tolkes at enkelte logikker fungerer bedre enn andre til ulike typer institusjonelt arbeid.

I starten av studien presenterte vi den overordnede problemstillingen:

> *Hvilke utfordringer står kommuner ovenfor når det gjelder informasjonssikkerhet?*

Vi har funnet utfordringer som blant annet består av press på ressurser, manglende ledelse, mangel på rutiner for arbeidet med ISS, vanskeligheter med å samarbeide og jobbe mot enkelte virksomheter i kommunen. Dette er også funn som bekrefter flere av de samme funnene som fremgår i rapporten fra Digitaliseringsdirektoratet (2020). Hadde vi ikke tatt i bruk den teoretiske linsen som er blitt brukt i studien hadde vi kun fått en deskriptiv beskrivelse av utfordringene. Derfor stilte vi følgende forskningsspørsmål:

> *Hva kan forklare utfordringene som kommunene står ovenfor når det gjelder informasjonssikkerhetsstyring?*

Institusjonelt arbeid og institusjonell logikk har bidratt til å forklare noen av utfordringene kommunene står ovenfor. Utfordringer er relatert til spenninger mellom logikker, institusjonell pluralisme, press på ressurser og manglende rutiner som hindrer institusjonelt arbeid. For at denne studien skulle få bedre nytte for praksis ønsket vi å komme med forslag til hvordan man kan imøtekomme disse utfordringene, og vi stilte derfor følgende forskningsspørsmål:

> *Hvordan kan kommunene imøtekomme noen av utfordringene med informasjonssikkerhetsstyring?*

For å imøtekomme utfordringene som ble identifisert, kan et nettverkssamarbeid som involverer aktører og virksomheter på tvers bidra til å skape en felles logikk som støtter ISS, større bevissthet, eierskap og kan føre til mer vellykket arbeid med ISS. Det bør også stilles spørsmål hvorvidt kommunen skal praktisere en sentralisert eller desentralisert tilnærming til styring. En desentralisert tilnærming kan støtte ISS bedre, men dette krever at det settes av tilstrekkelig med ressurser, definerte prosesser og jevnlige møter med nettverket slik at man har oversikt og kontroll over arbeidet med ISS. I de neste avsnittene vil vi forklare hvordan studien har implikasjoner for teori og praksis.

9.1 Implikasjoner for teori

Ulike logikker kan bidra til å forklare hvorfor det i noen virksomheter blir rapportert mer eller mindre avvik enn hos andre. Informantene forklarte at de hadde mest problemer med å få gjennomslagskraft hos skole og oppvekst. Logikkene som eksisterer blant dem, virker ikke til å støtte arbeidet med ISS og det kreves store institusjonelle endringer i disse virksomhetene. Videre har vi vist at logikker påvirker institusjonelt arbeid og vi identifiserte

at byråkratilogikk ikke sammenfalt godt med en desentralisert styring og nettverkssamarbeid. Samarbeidsaktiviteter kan være med på å endre disse logikkene, og i noen av kommunene vi undersøkte har nettverksamarbeid med stor sannsynlighet endret noen av logikkene og skapt en avvikskultur. Dette viser et eksempel på hvordan institusjonelt arbeid i form av "etablere normative nettverk" kan være med på å endre logikkene og dermed knytter begge disse teoriene sammen. ISS-logikk basert på verdier som samarbeid på tvers, deling av informasjon, positiv assosiasjon til avvik, og kontroll og revisjon ble presentert i studien som en ny logikk som støtter arbeidet med ISS. Denne logikken kunne bidra til å involvere kommunens virksomheter på en bedre måte og skape et mer vellykket arbeid med ISS. Verdiene, samt symbolske og materialistiske elementer vi har lagt til grunn for ISS-logikken og som således kan defineres som en idealtype kan tas i bruk i fremtidig forskning på ISS som bruker institusjonell logikk.

Vi har beskrevet måter individer bidrar til å endre logikker gjennom institusjonelt arbeid som består av blant annet: "etablere normative nettverk", "utdanning", "politiarbeid", "teoretisering" samt "innbaking og rutine". Institusjonelt arbeid har således vært nyttig i å forklare hvordan personer jobber med å endre institusjonen slik at den støtter ISS på en bedre måte. Det viste seg at personer ikke kun tar i bruk en type institusjonelt arbeid, men gjerne en kombinasjon i arbeidet med ISS. Funn i studien viser at institusjonelt arbeid i form av *forhindre institusjoner* ikke var til stede i arbeidet med ISS. Dette bekreftet antakelser i teorien om at denne typen institusjonelt arbeid sjeldent fremkommer. Hvilke betydninger og implikasjoner studien har for praksis blir beskrevet i det kommende avsnittet.

9.2 Implikasjoner for praksis

For praksis viser studien at arbeidet med ISS er komplisert. Blant annet er det ikke nødvendig å ta i bruk et rammeverk slavisk, men å forsøke å bruke dem så godt som mulig kan skape gevinster i form av bedre gjennomført arbeid med ISS. Rammeverket ISO27001, kan bidra til å få frem viktigheten med å ha en kontrollerende del. Uten denne delen kan ikke ISS forbedres eller fornyes, og man vil få mindre nytte av dette arbeidet. Tidligere rapporter, om ISS i norske kommuner, har kun fokusert på å beskrive hvilke utfordringer kommunene står ovenfor og ikke mulige løsninger. Denne studien har forklart årsaker til utfordringer og måter å imøtekomme disse utfordringene på inndelt i fire ulike ISS-komponenter. Våre anbefalinger til mulige løsninger er som følger:

- Revisjoner og kontroll er en viktig del av ISS og man må sørge for å gjennomføre revisjoner slik at man får kontroll over tilstanden til ISS og kontinuerlig kan forbedre dette arbeidet. Det hjelper også til å identifisere hvilket modenhetsnivå ISS befinner seg i. Man bør også sørge for å endre kulturen og tankegangen til ansatte om avvik, ved å aktivt innarbeide dette som noe positivt og forbedringsmuligheter. Avvik kan brukes til å måle tilstanden til ISS og indikerer rom for forbedringer.
- Eierskap bør sikres ved å aktivt involvere virksomhetene i arbeidet med, og utformingen av ISS og retningslinjer. En desentralisert tilnærming sørger for å plassere dette arbeidet ut i linjene og øke bevisstheten. Et nettverk kan være en måte for å samle virksomhetene og de involverte i dette arbeidet.
- Opplæring og sikkerhetskultur er viktig for en vellykket ISS og dette er noe ISS kan sørge for. Å gjøre opplæring til en del av rutinen i ledermøter og ansettelsesprosessen kan være nyttig. Samarbeidsaktiviterer gjennom jevnlige nettverksmøter er her også en gunstig tilnærming.

- Ansvar og roller må bli definert og komme tydelig frem. Uklare ansvar og roller er et hinder for arbeidet med ISS. Tilstrekkelig støtte og bevissthet hos toppledelsen kan bidra til å sikre at dette blir gjort. Det viser seg også å være nyttig å etablere og definere en egen informasjonssikkerhetsrolle.

Våre funn bekrefter det som kommer frem i rapporten fra Digitaliseringsdirektoratet, at små og mellomstore kommuner møter utfordringer i arbeidet med ISS. Utover dette viser våre funn at det er mulig for mindre kommuner å gjøre et godt arbeid med ISS så lenge ressurser blir bevilget og man har ansatte som er motivert for denne jobben. I tillegg vil definert prosesser bidra med å støtte arbeidet med ISS. Dette stemmer overens med forskningen som sier at definerte prosesser relateres til et høyere ISS-modenhetsnivå og støtter en desentralisert tilnærming til styring. Vi vil derfor anbefale prosesskartlegging som en god støtte til arbeidet med ISS.

Til slutt, identifiserte vi at ressurser var en av de største utfordringene som hindret arbeidet med ISS i kommunene. En gjenganger er at det ikke er bevilget tilstrekkelig ressurser til arbeidet med ISS, og at dette ikke får økt fokus før det skjer angrep slik som i Østre Toten. Dette viser en reaktiv tilnærming til informasjonssikkerhet. Det er viktig at kommuneledelsen er proaktive i sitt syn på informasjonssikkerhet og forstår viktigheten med informasjonssikkerhetsstyring og hvilken rolle den har i å bevare innbyggernes integritet. På den måten kan man, om ikke hindre, redusere omfanget av hendelser slik som i Østre Toten.

På en av de første sidene i studien presenterte vi et sitat av John F. Kennedy. Med dette håper vi leseren nå innser sitatets relevans og betydning, og som en siste oppfordring til kommuner i Norge vil vi derfor gjenta sitatet en siste gang:

> *"There are risks and costs to a program of action — but they are far less than the long-range cost of comfortable inaction."* John F. Kennedy, 35. Presidenten i Amerikas forente stater.

9.3 Videre forskning

Videre forskning bør ta i bruk andre forskningsdesign som Delphistudier, for å for eksempel stadfeste og bekrefte suksessfaktorer for vellykket ISS. Spørreskjema og kvantitative design vil også kunne bidra med forskning som kan generaliseres, og dette kan gjøres i kombinasjon med institusjonell teori. I tillegg bør man bidra med forskning som undersøker mer inngående i enkeltcaser hos kommuner, hvor man intervjuer personer på flere nivåer i kommunene. Forskning på ISS er et relativt underrepresentert felt og fremtidige forskningsbidrag vil bidra til å belyse dette feltet, hvilket vil gi nytte på et teoretisk og praktisk nivå. Studien har kun fokusert på offentlig sektor og det kan stilles spørsmål hvorvidt resultatene i studien kan overføres til privat sektor. Dette med tanke på det teoretiske grunnlaget og logikkene, ettersom det er sannsynlig at det eksister ulike logikker mellom privat og offentlig sektor, bør fremtidig forskning ta hensyn til dette.

Studien har bevist at institusjonell logikk og institusjonelt arbeid fungerer godt som teoretisk linse når man studerer ISS, og vi anbefaler derfor videre forskning å bygge videre på dette. Det ble funnet ulike typer institusjonelt arbeid som hadde vært interessant å undersøke om er typisk for arbeidet med ISS, og som kan bekrefte eller avkrefte noen av de samme funnene som i denne studien. Vi klarte ikke å identifisere alle typene institusjonelt arbeid som fremkom i teorien. Det hadde derfor vært interessant om videre forskning kan finne ut om dette kan forklares av datamaterialet eller om dette er institusjonelt arbeid som ikke passer for ISS. Det anbefales videre at fremtidig forskning tar for seg en induktiv tilnærming og

forsøker å identifisere nye logikker utover de etablerte logikkene. Til slutt, ville det vært interessant å undersøke om det finnes logikker tilsvarende ISS-logikken, og om de symbolske og materialistiske verdiene bak denne logikken også vil bekreftes i videre forskning.

Referanser

Ada, S., Sharman, R. & Gupta, M. (2009). Theories Used in Information Security Research: Survey and Agenda. I. https://doi.org/10.4018/978-1-60566-132-2

Ajer, A. K. S., Hustad, E. & Vassilakopoulou, P. (2021). Enterprise architecture operationalization and institutional pluralism: The case of the Norwegian Hospital sector. *Information Systems Journal*.

Albuquerque Junior, A. E. d. & Santos, E. M. d. (2015). Adoption of Information Security measures in public research institutes. *JISTEM-Journal of Information Systems and Technology Management*, *12*(2), 289-315.

AlGhamdi, S., Win, K. T. & Vlahu-Gjorgievska, E. (2020). Information security governance challenges and critical success factors: Systematic review. *Computers & Security*, *99*, 102030. https://doi.org/https://doi.org/10.1016/j.cose.2020.102030

Alharahsheh, H. & Pius, A. (2020). A review of key paradigms: Positivism VS interpretivism. *Global Academic Journal of Humanities and Social Sciences*, *2*(3), 39-43.

Alvesson, M., Hallett, T. & Spicer, A. (2019). Uninhibited institutionalisms. *Journal of management inquiry*, *28*(2), 119-127.

Alvesson, M. & Spicer, A. (2019). Neo-institutional theory and organization studies: a mid-life crisis? *Organization studies*, *40*(2), 199-218.

Andreas Krantz, Mette Finborud Børresen, Trond Ivan Hagen & Mo, A.-K. (2020, 02.09.2020). *Dataangrepet: Kan skade korona-beredskapen*. NRK. Hentet 16.02.2021 fra https://www.nrk.no/innlandet/10.000-kommuneansatte-rammet-av-dataangrep-1.15143964

Asnar, Y. & Massacci, F. (2011). A Method for Security Governance, Risk, and Compliance (GRC): A Goal-Process Approach. I A. Aldini & R. Gorrieri (Red.), *Foundations of Security Analysis and Design VI: FOSAD Tutorial Lectures* (s. 152-184). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-23082-0_6

Battilana, J. & Dorado, S. (2010). BUILDING SUSTAINABLE HYBRID ORGANIZATIONS: THE CASE OF COMMERCIAL MICROFINANCE ORGANIZATIONS. *The Academy of Management Journal*, *53*(6), 1419-1440. http://www.jstor.org/stable/29780265

Baxter, P. & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. *The qualitative report*, *13*(4), 544-559.

Becker, M. Y. (2007). Information governance in NHS's NPfIT: A case for policy specification. *International Journal of Medical Informatics*, *76*(5), 432-437. https://doi.org/https://doi.org/10.1016/j.ijmedinf.2006.09.008

Benbasat, I., Goldstein, D. K. & Mead, M. (1987). The case research strategy in studies of information systems. *MIS quarterly*, 369-386.

Berente, N. & Yoo, Y. (2012). Institutional Contradictions and Loose Coupling: Postimplementation of NASA's Enterprise Information System. *Information systems research*, *23*(2), 376-396. http://www.jstor.org/stable/23274429

Berg Johansen, C. & Waldorff, S. (2015). What are Institutional Logics - and Where is the Perspective Taking Us? *Academy of Management Proceedings*, *2015*, 14380-14380. https://doi.org/10.5465/AMBPP.2015.14380abstract

Berg, L. & Pinheiro, R. (2016). Handling Different Institutional Logics in the Public Sector: Comparing Management in Norwegian Universities and Hospitals. I (Bd. 45, s. 145-168). https://doi.org/10.1108/S0733-558X20150000045018

Besharov, M. & Smith, W. (2014). Multiple Institutional Logics in Organizations: Explaining Their Varied Nature and Implications. *Academy of Management Review*, *39*, 364-381. https://doi.org/10.5465/amr.2011.0431

Björck, F. (2004). *Institutional theory: a new perspective for research into IS/IT security in organisations*. https://doi.org/10.1109/HICSS.2004.1265444

Bowen, G. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, *9*, 27-40. https://doi.org/10.3316/QRJ0902027

Brandtzæg, B. A. L., Trond Erik , Aastvedt, A., Thorstensen, A., Groven, S. & Møller, G. (2019). *Utredning om små kommuner* (TF-rapport nr. 473). K.-o. moderniseringsdepartementet. https://www.regjeringen.no/contentassets/cc6fa29f7d0244059d62a98a4fdc5dfd/rapport_sma-kommuner_kmd_telemarksforsking-992102-l1000322.pdf

Bsigroup. (2018). *Information and Cyber Challenges in the Public Sector* (Report P.8). Bsigroup. https://www.bsigroup.com/globalassets/localfiles/en-ie/csir/resources/whitepaper/uk-engb-survey-wp-challenges-public-sector-cloud.pdf

Busch, P. A. (2018, Desember). *Technology and Institutional Logics*. The 39th International Conference on Information Systems (ICIS). San Francisco. https://www.researchgate.net/publication/328768406_Technology_and_Institutional_Logics

Busch, P. A. (2019). Digital Discretion Acceptance and Impact in Street-Level Bureaucracy.

Busch, T. & Ramstad, L. S. (2004). *Modernisering av offentlig sektor: endringsprosesser, legitimitet og løse koblinger*. Høgskolen i Sør-Trøndelag.

Carcary, M. (2009). The Research Audit Trial--Enhancing Trustworthiness in Qualitative Inquiry. *Electronic Journal of Business Research Methods*, *7*(1).

Carcary, M., Renaud, K., McLaughlin, S. & O'Brien, C. (2016). A framework for information security governance and management. *It Professional*, *18*(2), 22-30.

Connelly, L. M. (2016). Trustworthiness in qualitative research. *Medsurg Nursing*, *25*(6), 435.

Conner, F. W. & Coviello, A. W. (2004). Information security governance: A call to action. *The Corporate Governance Task Force*, 3-49.

Currie, W. (2009). Contextualising the IT artefact: towards a wider research agenda for IS using institutional theory. *Information Technology & People*.

Currie, W. L. & Guah, M. W. (2007). Conflicting institutional logics: a national programme for IT in the organisational field of healthcare. *Journal of Information Technology*, *22*(3), 235-247. https://doi.org/10.1057/palgrave.jit.2000102

Dang, D. (2021). Institutional Logics and Their Influence on Enterprise Architecture Adoption. *Journal of Computer Information Systems*, *61*(1), 42-52. https://doi.org/10.1080/08874417.2018.1564632

Datatilsynet. (2018, 30.10.2018). *Etablere internkontroll*. Hentet 20.02.2021 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Datatilsynet. (2019, 20.03.2019). *Felles løft for informasjonssikkerhet i skolesektoren*. Hentet 20.02.2021 fra https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-20192/felles-loft-for-informasjonssikkerheten-i-skolesektoren/

Datatilsynet. (u.å). *Informasjonssikkerhet og internkontroll*. Hentet 20.02.2021 fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/

Death, D. (2017). *Information security handbook: develop a threat model and incident response strategy to build a strong information security framework* (1st ed. utg.). Birmingham: PACKT Publishing.

Departementene. (2019). *Nasjonal strategi for digital sikkerhet* (G-0444 B). Regjeringen. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf
Digdir. (2020, 30.11.2020). *Behov for å styrke informasjonssikkerheten i fylkeskommuner og kommuner*. Hentet 24.02.2021 fra https://www.digdir.no/informasjonssikkerhet/behov-styrke-informasjonssikkerheten-i-fylkeskommuner-og-kommuner/2128
Digdir. (u.å-a). *Fellestrekk for styring og kontroll*. Hentet 22.04.2021 fra https://www.digdir.no/informasjonssikkerhet/fellestrekk-styring-og-kontroll/2278
Digdir. (u.å-b). *Hva vil det si å jobbe helhetlig?* Hentet 22.04.2021 fra https://www.digdir.no/informasjonssikkerhet/hva-vil-det-si-jobbe-helhetlig/2277
Digdir. (u.å-c). *Infromasjonssikkerhet - en forutsetning for å nå virksomhetens mål* Hentet 20.03.2021 fra https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123
Digdir. (u.å-d). *Internkontroll/styringssystem/ledelsessystem for informasjonssikkerhet*. Hentet 20.03.2021 fra https://www.digdir.no/digitale-felleslosninger/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet/1490
Digdir. (u.å-e). *Styring og kontroll*. Hentet 20.02.2021 fra https://www.digdir.no/informasjonssikkerhet/styring-og-kontroll/1161
Digdir. (u.å-f). *Systematiske aktiviteter*. Hentet 09.04.2021 fra https://internkontroll-infosikkerhet.difi.no/systematiske-aktiviteter
Digitaliseringsdirektoratet. (2020). *Arbeidet med informasjonssikkerhet i fylkeskommuner og kommuner* (Digdir-rapport ISSN 2703-7061). Digdir. https://www.digdir.no/informasjonssikkerhet/arbeidet-med-informasjonssikkerhet-i-fylkeskommuner-og-kommuner/2102
Digitaliseringsdirektoratet. (u.å). *Regelverkskravet*. Difi. Hentet 20.02.2021 fra https://internkontroll-infosikkerhet.difi.no/regelverkskrav
DiMaggio, P. J. & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American sociological review*, 147-160.
DiMaggio, P. J. & Powell, W. W. (1991). *The New institutionalism in organizational analysis*. University of Chicago Press.
Direktoratet for e-helse. (2019). *Informasjonssikkerhet i helse- og omsorgssektoren 2019* (IE-1054). https://ehelse.no/publikasjoner/informasjonssikkerhet-i-helse-og-omsorgstjenesten-2019
eForvaltningsforskriften. (2004). *Forskrift om elektronisk kommunikasjon med og i forvaltningen* (FOR-2004-06-25-988). Lovdata. https://lovdata.no/dokument/SF/forskrift/2004-06-25-988
Fàbregues, S. & Fetters, M. D. (2019). Fundamentals of case study research in family medicine and community health. *Family medicine and community health*, *7*(2).
Fazlida, M. R. & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, *28*, 243-248. https://doi.org/https://doi.org/10.1016/S2212-5671(15)01106-5
Fiss, P. C. (2008). Institutions and corporate. I *The Sage handbook of organizational institutionalism* (Bd. 389).
Fred, M. (2020). Local government projectification in practice–a multiple institutional logic perspective. *Local Government Studies*, *46*(3), 351-370.
Friedland, R. & Alford, R. (1991). Bringing Society Back In. I.
Gashgari, G., Walters, R. J. & Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance. IoTBDS,

Gawer, A. & Phillips, N. (2013). Institutional Work as Logics Shift: The Case of Intel's Transformation to Platform Leader. *Organization studies*, *34*(8), 1035-1071. https://doi.org/10.1177/0170840613492071
Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal*.
Guba, E. G. & Lincoln, Y. S. (1989). *Fourth generation evaluation*. Sage.
Gullberg, C. & Svensson, J. (2020). Institutional Complexity in Schools: Reconciling Clashing Logics Through Technology? *Scandinavian Journal of Public Administration*, *24*.
Hansen, T. (2018, 17.09.2018). *New Public Management*. Store norske leksikon. Hentet 23.04.2021 fra https://snl.no/New_Public_Management
Haqaf, H. & Koyuncu, M. (2018). Understanding key skills for information security managers. *International Journal of Information Management*, *43*, 165-172. https://doi.org/https://doi.org/10.1016/j.ijinfomgt.2018.07.013
Harrison, H., Birks, M., Franklin, R. & Mills, J. (2017). Case study research: Foundations and methodological orientations. Forum Qualitative Sozialforschung/Forum: Qualitative Social Research,
Heredia, H. & Merchán, V. (2020). Towards the Information Security Governance for Institutions of Higher Education: Harmonization of Standards. I M. Botto-Tobar, M. Zambrano Vizuete, P. Torres-Carrión, S. Montes León, G. Pizarro Vásquez & B. Durakovic, *Applied Technologies* Cham.
Holgate, J., Williams, S. & Hardy, C. (2012). Information Security Governance: Investigating Diversity in Critical Infrastructure Organizations.
Hyett, N., Kenny, A. & Dickson-Swift, V. (2014). Methodology or method? A critical review of qualitative case study reports. *International journal of qualitative studies on health and well-being*, *9*, 23606-23606. https://doi.org/10.3402/qhw.v9.23606
Irani, Z., Ezingeard, J.-N., Grieve, R. & Race, P. (1999). A case study strategy as part of an information systems research methodology: a critique. *International Journal of Computer Applications in Technology*, *12*(2-5), 190-198.
IT Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (ISBN 1-933284-29-3). https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf
Jacobsen, D. I. (2010). *Forståelse, beskrivelse og forklaring*. Høyskoleforlaget.
Jacobsen, D. I. (2015). *Hvordan gjennomføre undersøkelser?* Cappelen Damm akademisk.
Kallio, H., Pietilä, A. M., Johnson, M. & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing*, *72*(12), 2954-2965.
Kandathil, G., Wagner, E. & Newell, S. (2011). Translating ES-embedded institutional logics through technological framing: An Indian-based case example.
Kaplan, B. & Maxwell, J. A. (2005). Qualitative Research Methods for Evaluating Computer Information Systems. I J. G. Anderson & C. E. Aydin (Red.), *Evaluating the Organizational Impact of Healthcare Information Systems* (s. 30-55). Springer New York. https://doi.org/10.1007/0-387-30329-4_2
Kommunal- og moderniseringsdepartementet. *Statlig styring av kommuner og fylkeskommuner - Med prinsipper og retningslinjer* (H-2477 B). Regjeringen. https://www.regjeringen.no/contentassets/8d68861d5d014c6ab4183f9f77137760/no/pdfs/veileder-om-statlig-styring-av-kommunesektoren-med.pdf
Kommunesektorens organisasjon. (u.å). *Digitaliseringsstrategi for kommuner og fylkeskommuner* (ISBN 978-82-93199-19-05). Kommunesektorens organisasjon.

https://www.ks.no/globalassets/fagomrader/digitalisering/klart-sprak-i-digitale-selvbetjeningslosninger/sprak-og-tekst/ingresser/KS-Digitaliseringsstrategi-hefte-F32.pdf
Kristiansen, M., Obstfelder, A. & Lotherington, A. T. (2015). Nurses' sensemaking of contradicting logics: An underexplored aspect of organisational work in nursing homes. *Scandinavian Journal of Management*, *31*(3), 330-337. https://doi.org/https://doi.org/10.1016/j.scaman.2015.04.003
KS. (2021, 11.01.2021). *Vær oppmerksom på sikkerheten etter dataangrep i Østre Toten*. KS. Hentet 17.02.2021 fra https://www.ks.no/fagomrader/digitalisering/styring-og-organisering/oppfolging-av-dataangrepet-i-ostre-toten/
Lammers, J. & Garcia, M. (2017). Institutional Theory Approaches. I. https://doi.org/10.1002/9781118955567.wbieoc113
Langley, A. & Royer, I. (2006). Perspectives on doing case study research in organizations. *M@n@gement*, *9*(3), 81-94.
Lawrence, T., Suddaby, R. & Leca, B. (2011). Institutional work: Refocusing institutional studies of organization. *Journal of management inquiry*, *20*(1), 52-58.
Lawrence, T. B., Leca, B. & Zilber, T. B. (2013). Institutional work: Current research, new directions and overlooked issues. *Organization studies*, *34*(8), 1023-1033.
Lawrence, T. B. & Suddaby, R. (2006). 1.6 institutions and institutional work. *The Sage handbook of organization studies*, 215-254.
Lidster, W. & Rahman, S. (2018). *Obstacles to Implementation of Information Security Governance*. https://doi.org/10.1109/TrustCom/BigDataSE.2018.00276
Lounsbury, M. (2007). A tale of two cities: Competing logics and practice variation in the professionalizing of mutual funds. *Academy of management journal*, *50*(2), 289-307.
Love, P., Reinhard, J., Schwab, A. J. & Spafford, G. (2010). *Global Technology Audit Guide (GTAG) 15 - Information Security Governance*. The Institute of Internal Auditors. https://www.iia.nl/SiteFiles/IIA_leden/Praktijkgidsen/GTAG-15%20Information%20Security%20Governance.pdf
Maynard, S. B., Tan, T., Ahmad, A. & Ruighaver, T. (2018). Towards a Framework for Strategic Security Context in Information Security Governance. *Pacific Asia journal of the Association for Information Systems*, 65-88. https://doi.org/10.17705/1PAIS.10403
Meyer, R. E., Egger-Peitler, I., Höllerer, M. A. & Hammerschmid, G. (2014). Of bureaucrats and passionate public managers: Institutional logics, executive identities, and public service motivation. *Public Administration*, *92*(4), 861-885.
Mishra, S. (2015). Organizational objectives for information security governance: a value focused assessment. *Information & Computer Security*.
Moulton, R. & Coles, R. S. (2003). Applying information security governance. *Computers & Security*, *22*(7), 580-584. https://doi.org/https://doi.org/10.1016/S0167-4048(03)00705-3
Mukundan, N. R., Mukundan, N. R., Prakash Sai, L. & Prakash Sai, L. (2014). Perceived information security of internal users in Indian IT services industry. *Information technology and management*, *15*(1), 1-8. https://doi.org/10.1007/s10799-013-0156-y
Musa, N. (2018). A Conceptual Framework of IT Security Governance and Internal Controls. 2018 Cyber Resilience Conference (CRC),
Myers, M. D. & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and organization*, *17*(1), 2-26.
Norges Kommunerevisorforbund. (2021). *KS oppfordrer kommunene til å være oppmerksom på sikkerheten etter dataangrep*. Hentet 17.02.2021 fra

https://www.nkrf.no/nyheter/2021/01/12/ks-oppfordrer-kommunene-til-a-vaere-oppmerksom-pa-sikkerheten-etter-dataangrep
NorSIS. (u.å). *Kommune CERT - utredning av behov og muligheter*. https://norsis.no/d18ba623c92d1ded748a61ae70/KommuneCSIRT_print.pdf
NSD. (u.å-a). *Fylle ut meldeskjema for personopplysninger*. Hentet 28.01.2021 fra https://www.nsd.no/personverntjenester/fylle-ut-meldeskjema-for-personopplysninger/
NSD. (u.å-b). *Om NSD - Norsk senter for forskningsdata*. Hentet 28.01.2021 fra https://www.nsd.no/om-nsd-norsk-senter-for-forskningsdata/
NTB. (2019, 29.04.2019). *En av ti norske kommuner har vært utsatt for dataangrep det siste året*. Aftenposten. Hentet 17.02.2021 fra https://www.aftenposten.no/norge/i/1noApB/en-av-ti-norske-kommuner-har-vaert-utsatt-for-dataangrep-det-siste-aaret
NTB. (2020, 02.09.2020). *Riksrevisjonen: Norge er dårlig beskyttet mot hackerangrep*. Indre Akershus Blad. Hentet 17.02.2021 fra https://www.indre.no/riksrevisjonen-norge-er-darlig-beskyttet-mot-hackerangrep/s/5-25-283022
NTB. (2021, 18.01.2021). *NSM advarer kommuner og offentlig sektor om løspengevirus*. Digi. Hentet 17.02.2021 fra https://www.digi.no/artikler/nsm-advarer-kommuner-og-offentlig-sektor-om-losepengevirus/505669
Nærø, A. F. (2020, 09.02.2020). *Datatilsynet slår alarm om IT-sikkerhet i skolene*. E24. Hentet 24.02.2021 fra https://e24.no/teknologi/i/opzXrV/datatilsynet-slaar-alarm-om-it-sikkerhet-i-skolene.
Oates, B. J. (2006). *Researching Information Systems and Computing.* SAGE Publications.
Okoli, C. (2015). A guide to conducting a standalone systematic literature review. *Communications of the Association for Information Systems*, *37*(1), 43.
Patton, M. Q. (1990). *Qualitative evaluation and research methods*. SAGE Publications, inc.
Peterson, R. (2004). Crafting Information Technology Governance. *Information systems management*, *21*(4), 7-22. https://doi.org/10.1201/1078/44705.21.4.20040901/84183.2
Poore, R. S. (2005). Information Security Governance. *EDPACS*, *33*(5), 1-8. https://doi.org/10.1201/1079.07366981/45653.33.5.20051101/91005.1
Posthumus, S. & von Solms, R. (2004). A framework for the governance of information security. *Computers & Security*, *23*(8), 638-646. https://doi.org/https://doi.org/10.1016/j.cose.2004.10.006
PST. (u.å). *Nasjonal trusselvurdering 2021*. Hentet 22.04.2021 fra https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2021/#Innledning
Rannenberg, K., Varadharajan, V. & Weber, C. (2010). *Security and Privacy–Silver Linings in the Cloud*. Springer.
Reay, T. & Hinings, C. R. (2009). Managing the rivalry of competing institutional logics. *Organization studies*, *30*(6), 629-652.
Reay, T. & Jones, C. (2016). Qualitatively capturing institutional logics. *Strategic Organization*, *14*(4), 441-454. https://doi.org/10.2307/26369319
Rebollo, O., Mellado, D., Sánchez Crespo, L. E. & Fernández-Medina, E. (2011). *Comparative Analysis of Information Security Governance Frameworks: A Public Sector Approach*.
Regjeringen. (u.å). *Kommunereform*. Hentet 25.01.2021 fra https://www.regjeringen.no/no/tema/kommuner-og-regioner/kommunereform/id751048/
Rogaland Revisjon IKS. (2019). Forvaltningsrevisjon av informasjonssikkerhet, drift og sårbarhet. https://www.rogaland-

revisjon.no/userfiles/upload/files/import/rr%20sandnes%202019%20informasjonssikkerhet%2c%20drift%20og%20sårbarhet.pdf
Røgeberg, O. (2019, 29.04.2019). *Offentlig sektor sliter med rekruttering av IKT-spesialister*. Statistisk sentralbyrå. Hentet 16.04.2021 fra
Sandefjord kommune. (u.å). *Informasjonssikkerhet og personvern - overordnet styringsdokument* S. kommune. https://www.sandefjord.kommune.no/globalassets/sandefjordbeta/overordnet-styringsdokument-informasjonssikkerhet.pdf
Sanders, P. (2019, 21.08.2019). *Key cybersecurity threats in the public sector*. identifi global. Hentet 17.02.2021 fra https://www.identifiglobal.com/news/key-cybersecurity-threats-in-the-public-sector/39972/
Schinagl, S. (2020). What do we know about information security governance?'From the basement to the boardroom': Towards digital security governance. *Res. IT-Auditing Multidisciplinary View Ed.*, 135.
Schinagl, S. & Shahim, A. (2020). What do we know about information security governance? *Information & Computer Security*.
Schoch, K. (2016). Case study research. *The scholar-practitioner's guide to research design*, *1*, 5886-6283.
Schreier, M. (2014). The SAGE Handbook of Qualitative Data Analysis. I. SAGE Publications Ltd. https://doi.org/10.4135/9781446282243
Scott, W. R. (2001). *Institutions and organizations* (2nd ed. utg.). Sage Publications.
Sgourev, S. V. (2011). "Wall Street" meets Wagner: Harnessing institutional heterogeneity. *Theory and society*, *40*(4), 385-416.
Sigrid Gausen, Torgeir Knutsen, Solveig Ruud & Strandberg, T. (2021, 11.03.2021). *Stortinget utsatt for IT-angrep: «Et angrep på vårt demokrati»*. Aftenposten. Hentet 17.03.2021 fra https://www.aftenposten.no/norge/i/PRnGRX/stortinget-utsatt-for-it-angrep-et-angrep-paa-vaart-demokrati
Siponen, M. & Willison, R. (2009). Information security management standards: Problems and solutions. *Information & Management*, *46*(5), 267-270. https://doi.org/https://doi.org/10.1016/j.im.2008.12.007
Slayton, R. (2021). Governing Uncertainty or Uncertain Governance? Information Security and the Challenge of Cutting Ties. *Science, Technology, & Human Values*, *46*(1), 81-111. https://doi.org/10.1177/0162243919901159
Solbakken, H. A. (2020, 10.01.2021). *Sensitiv pasientinformasjon kan være på avveie etter dataangrep*. NRK. Hentet 15.01.2021 fra https://www.nrk.no/innlandet/ostre-toten-kommune-angrepet-av-hackere-_-pasientinformasjon-og-helsedata-kan-vaere-pa-avveie-1.15321398
Stake, R. E. (1995). *The art of case study research*. sage.
Statens innkrevingssentral. (u.å). *Hjemmel*. Hentet 03.03.2021 fra https://www.sismo.no/no/pub/ordforklaringer/hjemmel
Statistisk sentralbyrå. (2016). *Regler for inndeling av kommunal virksomhet i Enhetsregisteret*. S. sentralbyrå. https://www.ssb.no/innrapportering/offentlig-sektor/_attachment/295798?_ts=15a37dd1868
Stoll, M. (2013). Development of Stakeholder Oriented Corporate Information Security Objectives. I K. Elleithy & T. Sobh, *Innovations and Advances in Computer, Information, Systems Sciences, and Engineering* New York, NY.
Sørgård, J. (2013). *Styringssystem for informasjonssikkerhet - et topplederansvar og en viktig kulturpåvirker*. Hentet 24.02.2021 fra https://www.uninett.no/sites/default/files/webfm/Styringssystem%20for%20informasjonssikkerhet%20-%20Jan%20Sørgård%2C%20Difi.pdf

Tan, T. C. C., Ruighaver, A. B. & Ahmad, A. (2010). Information Security Governance: When Compliance Becomes More Important than Security. I K. Rannenberg, V. Varadharajan & C. Weber, *Security and Privacy – Silver Linings in the Cloud* Berlin, Heidelberg.
Tan, T. H., Maynard, S. B., Ahmad, A. & Ruighaver, T. (2017). Information Security Governance: A Case Study of the Strategic Context of Information Security. PACIS,
Thorbjørnsrud, K., Figenschou, T. & Ihlen, Ø. (2014). Mediatization in public bureaucracies: A typology. *Communications*, *39*, 3-22. https://doi.org/10.1515/commun-2014-0002
Thornton, P. H. & Ocasio, W. (2008). Institutional logics. *The Sage handbook of organizational institutionalism*, *840*(2008), 99-128.
Thornton, P. H., Ocasio, W. & Lounsbury, M. (2012). *The Institutional Logics Perspective - A New Approach to Culture, Structure, and Process*. Oxford University Press.
Trondal, J. (2011). Bureaucratic structure and administrative behaviour: Lessons from international bureaucracies. *West European Politics*, *34*(4), 795-818.
UiA. (2020, 23.10.2020). *Information Systems* Hentet 22.01.2021 fra https://libguides.uia.no/c.php?g=430882&p=4596219
UiA. (u.å). *Forskningsetikk*. Hentet 19.04.2021 fra https://www.uia.no/for-ansatte/forskning/forskningsetikk
Veiga, A. D. & Eloff, J. H. (2007). An information security governance framework. *Information systems management*, *24*(4), 361-372.
von Solms, B. & von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, *23*(5), 371-376. https://doi.org/https://doi.org/10.1016/j.cose.2004.05.002
von Solms, R., Thompson, K.-L. & Maninjwa, M. (2011, 15-17 Aug. 2011). *Information security governance control through comprehensive policy architectures*. Information Security for South Africa (ISSA), Johannesburg, South Africa. https://ieeexplore.ieee.org/document/6027522
von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/https://doi.org/10.1016/j.cose.2013.04.004
von Solms, R. & von Solms, S. H. (2006). Information Security Governance: A model based on the Direct–Control Cycle. *Computers & Security*, *25*(6), 408-412. https://doi.org/https://doi.org/10.1016/j.cose.2006.07.005
Wahid, F. & Sein, M. K. (2013). Institutional entrepreneurs: The driving force in institutionalization of public systems in developing countries. *Transforming Government: People, Process and Policy*.
Walsham, G. (1995). Interpretive case studies in IS research: nature and method. *European Journal of information systems*, *4*(2), 74-81.
Webster, J. & Watson, R. T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS quarterly*, xiii-xxiii.
Whitman, M. & Mattord, H. (2014). Information Security Governance for the Non-security Business Executive. *11*, 97-111.
Whitman, M. E. & Mattord, H. J. (2011). *Principles of information security*. Cengage Learning.
Williams, P. (2008). In a 'trusting' environment, everyone is responsible for information security. *Information Security Technical Report*, *13*(4), 207-215. https://doi.org/https://doi.org/10.1016/j.istr.2008.10.009
Williams, S. P., Hardy, C. A. & Holgate, J. A. (2013). Information security governance practices in critical infrastructure organizations: A socio-technical and institutional

logic perspective. *Electronic Markets*, *23*(4), 341-354. https://doi.org/10.1007/s12525-013-0137-3
Wu, S. M., Guo, D. & Wu, Y. C. (2018). The Effects of Bank Employees' Information Security Awareness on Performance of Information Security Governance. I F. Xhafa, S. Patnaik & A. Y. Zomaya, *Advances in Intelligent Systems and Interactive Applications* Cham.
Xiao, Y. & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of Planning Education and Research*, *39*(1), 93-112.
Yaokumah, W. (2014). Information security governance implementation within Ghanaian industry sectors: An empirical study. *Information Management & Computer Security*, *22*(3), 235-250. https://doi.org/10.1108/IMCS-06-2013-0044
Yassine, M. & Abdelkebir, S. (2017). CAFISGO: a Capability Assessment Framework for Information Security Governance in Organizations. *12*, 209-217.
Yin, R. K. (2003). *Case Study Research*. SAGE.
Yin, R. K. (2014). *Case study research : design and methods* (fifth. utg.). SAGE Publications.
Zilber, T. B. (2013). Institutional logics and institutional work: should they be agreed? I *Institutional logics in action, Part A*. Emerald Group Publishing Limited.

Vedlegg

Vedleggsfortegnelse

Vedlegg 1: Intervjuguide

Intervjuguide kommuner

Type intervju (virtuelt/fysisk):

Intervjuets lengde:
Digitalt opptak eller lignende:

Form for transkripsjon:

Formål med prosjektet/masteroppgaven: Å oppnå kunnskap om hvordan informasjonssikkerhetsstyring og internkontroll blir praktisert i kommuner.

Vi starter med å informere deltakeren om vi får bruke opptak og at digitale opptak vil lagres trygt. Spør om det er greit om vi tar i bruk sitater fra intervjuet uten å nevne ditt eller kommunens navn.

- Ønsker du å lese gjennom rapporten før innlevering av oppgaven?

Bakgrunn og informasjon om intervjuobjektet

- Hvilken bakgrunn har du? Utdannelse, yrkeserfaring.
- Hva er din nåværende stilling, ditt arbeidsområde og hvor lenge har du jobbet i denne posisjonen?
- Hvor mange ansatte er det i denne avdelingen?
- Hvordan er avdelingen bygd opp/ansvarsområder?
- Tidligere roller/verv i denne kommunen?

Praksiser/logikker - narrativ fortelling

Informasjonssikkerhetsstyring:

- Kan du fortelle hvordan dere jobber med informasjonssikkerhetsstyring og internkontroll i kommunen?
- Er informasjonssikkerhetsstyring et eget område eller er det en del av IT/virksomhetsstyring?
- Hvem jobber med å utarbeide retningslinjer? Styringsdokumenter? Systemer?
- Hvem har ansvar for at informasjonssikkerheten blir ivaretatt?
- faggruppe/sikkerhetsleder/rådmann/ol?
- Hva er dine opplevelser med informasjonssikkerhetsstyring og internkontroll? Både fordeler og utfordringer.
- Ser du for deg at andre i kommunen opplever andre utfordringer?
- Hvordan jobber dere med risikostyring f.eks i et prosjekt, anskaffelse eller liknende?
- har dere utfordringer med dette? Forklar? Hva er det som evt. går bra?
- Har dere et hendelsesrapporteringssystem? Utfordringer med dette? Hva er bra?
- Evaluerer/reviderer dere retningslinjer og policier? Når gjøres dette? Hvem er med på dette arbeidet?

- Hva er dine synspunkter på informasjonssikkerhet i kommunen?

- Føler du informasjonssikkerheten blir ivaretatt?

- Har dere tidligere vært utsatt for angrep/trusler.

- Hvis ja, hva gjorde dere? hva lærte dere fra angrepet? Ble noe endret?

- Har dere interkommunalt samarbeid når det gjelder informasjonssikkerhet?

- Er dere sertifisert i noen sikkerhetsstandard? Som ISO. Etc.

Utvikling

- Hvordan jobbet dere med informasjonssikkerhetsstyring og internkontroll før? (hvis personen har jobbet der lenge nok) har noe endret seg?

- Hvordan ser du for deg at utviklingen med informasjonssikkerhetsstyring og internkontroll kommer til å skje de neste 10 årene? (Er det noe du synes er bra eller dårlig? hva trenger vi mer kunnskap om?)

Avslutning – noe som ikke er dekket?

- **Føler du det er noe som ikke er dekket i løpet av intervjuet, eller noe du gjerne vil diskutere før vi avslutter?**

Avslutter intervjuet med å takke for informasjonen og avtaler eventuelt oppfølgingsintervju, avklarer eventuell tilgang til intern informasjon (prosjektdokumenter, intranett osv.). Avklarer om informanten kan se gjennom sammendraget/transkriptet av intervjuet i ettertid for å oppklare eventuelle misforståelser.

Vedlegg 2: Samtykkeskjema

Forespørsel om deltakelse i forskningsprosjektet

«informasjonssikkerhetsstyring i kommunesektoren»

Dette er et spørsmål til deg om å delta i et forskningsprosjekt hvor formålet er å undersøke hvordan informasjonssikkerhetsstyring blir praktisert i kommunene. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål
Vi er to studenter som studerer master i informasjonssystemer og skriver masteroppgave ved fakultet for samfunnsvitenskap, institutt for informasjonssystemer på Universitetet i Agder. Formålet med oppgaven/studien er å få innsikt i hvordan kommuner praktiserer informasjonssikkerhetsstyring. I tillegg ønsker vi å finne hvilke utfordringer som man møter og komme med ulike forslag til løsninger. Forskningsspørsmålene vi ønsker å belyse er:

«Hvilke utfordringer står kommuner ovenfor når det gjelder informasjonssikkerhet?»

«Hva kan forklare utfordringene som kommunene står ovenfor når det gjelder informasjonssikkerhetsstyring?»

«Hvordan kan kommunene imøtekomme noen av utfordringene med informasjonssikkerhetsstyring?»

Gjennom innsamling av data fra intervjuer med ansatte i en eller flere kommuner vil vi kunne belyse disse problemstillingene og tilføre ny kunnskap til et viktig og aktuelt tema.

Vi ønsker å velge ut akkurat deg som deltaker ettersom du har relevant kunnskap å bidra med til oppgaven og som vil forme våre modeller og konklusjoner. I tillegg jobber du daglig med problemstillingene som vi ønsker å belyse. Din kunnskap og informasjonen du bidrar med vil være med på å besvare oppgavens problemstilling og bidra til ny interessant kunnskap innenfor et tidsriktig og viktig tema.

Hvem er ansvarlig for forskningsprosjektet?
Universitetet i Agder Kristiansand, fakultet for samfunnsvitenskap, institutt for informasjonssystemer er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?
Utvalget vil bli basert på kontakter vi har fått gjennom epost korrespondanse med kommuner og deres kontaktnettverk. I tillegg til at respondenten har erfaring om informasjonssikkerhetsstyring.

Hva innebærer det for deg å delta?
En kvalitativ metode med intervjuer vil bli brukt for å belyse problemstillingen. Intervjuet vil vare 45-60 minutter der vi vil spørre deg om det er greit vi tar opptak og notater. Intervjuet vil bli transkribert og lagret trygt i henhold til personvernlovgivning og slik at ingen uvedkommende vil få tilgang.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg. Deltakelse vil ikke påvirke ditt forhold til arbeidsgiver og arbeidsplassen.

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

- Veiledere og studentene som skriver denne oppgaven er de eneste som vil ha tilgang til dataene.
- Dataene vil bli sikret ved å bli lagret på universitetets servere med tilgangskontroll og loggføring.
- Navn og kontaktopplysninger vil ikke bli spurt om eller lagret.
- Deltakeren vil ikke kunne gjenkjennes i publikasjonen, kun opplysninger som stillingstittel og eventuelt størrelse på kommunen.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene og dataene slettes når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 09.06.2021.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene,
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

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

På oppdrag fra Universitetet i Agder Kristiansand, fakultet for samfunnsvitenskap, institutt for informasjonssystemer har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:

Student:

Mari Charlotte Åstrøm Holm

Masterstudent i Informasjonssystemer ved Universitetet i Agder

Tlf: 90734730

Mari.440@hotmail.com

Student:

Erling Tobias Skalleberg

Masterstudent i Informasjonssystemer ved Universitetet i Agder

Tlf: 94790138

erlingtob1@hotmail.com

Veileder:

Carl Erik Moe

Dosent/instituttleder ved institutt for informasjonssystemer, Universitetet i Agder

Tlf: +4738141796

carl.e.moe@uia.no

Veileder:

Geir Inge Hausvik

Førstemanuensis, Universitetet i Agder

Tlf: +4791565456

geir.i.hausvik@uia.no

Vårt personvernombud:

Ina Danielsen

Tlf: 45254401

personvernombud@uia.no

Adresse: Personvernombud ved Universitetet i Agder, Postboks 422, 4604 Kristiansand

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:

- NSD – Norsk senter for forskningsdata AS på epost (personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen

Prosjektansvarlig *Eventuelt student*

(Forsker/veileder)

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet [informasjonssikkerhetsstyring i kommuner], og har fått anledning til å stille spørsmål. Jeg samtykker til:

- ☐ å delta i [intervjuet]

Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet

---

(Signert av prosjektdeltaker, dato)

Vedlegg 3: Oversikt over data og konseptdrevne kategorier, samt hovedtema hentet fra NVivo

Institusjonelle logikker	
Hovedkategorier	Underkategorier
Byråkratilogikk	Ansvarsroller
	Hierarkisk
	Kontroll
	Lover & regler
	Prosedyre
	Sentralisert system
Markedslogikk	Fleksibilitet
	Innovasjon
	Resultatbasert
	Ytelse & effektivitet
	Økonomisk rasjonell
Profesjonslogikk	Autonomi
	Profesjonell assosiasjon
	Profesjonelle nettverk
	Status & ekspertise
	Verdier
ISS-logikk	Samarbeid på tvers
	Deling av informasjon
	Positiv assosiasjon til avvik
	Kontroll og revisjon
Institusjonelt arbeid	
Forstyrre institusjoner	Frakoble sanksjoner
	Frakoble moralske grunnlag
	Undergrave antagelser og tro
Ivareta institusjoner	Avskrekking
	Innbaking og rutine
	Muliggjøre arbeid
	Mytologisering
	Politiarbeid
	Valorisering og demonisering
Skape institusjoner	Beslutningspåvirkning
	Endring av normative assosiasjoner
	Etablere identiteter
	Etablere normative nettverk
	Definere
	Utdanning
	Mimikk
	Teoretisering
	Muliggjøre arbeid
Informasjonssikkerhetsstyring	
Utfordringer	Ansvar og roller
	Avvik
	Eierskap
	Opplæring
	Ressurser
	Revisjoner og kontroll
	Sikkerhetskultur

	Styringsmodell
	Toppledelsen
Fremmere	Arbeid på tvers
	Desentralisert styring
	Forbedrings og avvikskultur
	God opplæring
	Informasjonsdeling
	Kontrollsystem
	Lav terskel for avviksmeldinger
	Nedenfra opp
	Prosessledelse
	Standarder
	Tydelige ansvar og roller

Vedlegg 4: Vurdering av meldeskjema, NSD

Melding
14.12.2020 07:29

Det innsendte meldeskjemaet med referansekode 239910 er nå vurdert av NSD.

Følgende vurdering er gitt:

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 14.12.2020, samt i meldingsdialogen mellom innmelder og NSD. Behandlingen kan starte.

26.01.2021 - Vurdert
NSD har vurdert endringen registrert 19.01.2021

Vi har nå registrert 09.06.2021 som ny sluttdato for behandling av personopplysninger.

NSD vil følge opp ved ny planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til videre med prosjektet!

Kontaktperson hos NSD: Simon Gogl
Tlf. Personverntjenester: 55 58 21 17 (tast 1)