Universitetet i Stavanger

Kvalitet på tjenesteutsetting av digitale IKT tjenester i offentlig sektor

Er offentlig sektor forberedt

- Null eller full kontroll?

En studie på kvalitet på risiko og hvilken risikostyring det er ved digital IKT tjenesteutsetting i offentlig sektor

Anne Marie Dalen Øverhaug

Vår 2019

MASTERGRADSSTUDIUM I
RISIKOSTYRING OG SIKKERHETSLEDELSE

MASTEROPPGAVE

SEMESTER: Vår 2019

FORFATTER: Anne Marie Dalen Øverhaug

VEILEDER: Ole Andreas Hegland Engen

TITTEL PÅ MASTEROPPGAVE:

Kvalitet på tjenesteutsetting av digitale IKT tjenester i offentlig sektor
Er offentlig sektor forberedt - Null eller full kontroll?

En studie på kvalitet på risiko og hvilken risikostyring det er ved digital IKT tjenesteutsetting i offentlig sektor.

EMNEORD/STIKKORD: Kvalitet, tjenesteutsetting, offentlig sektor, risiko, risikofaktorer, risikostyring, risikovurdering, bestillerkompetanse, krav til IKT-tjenesten, beslutningstaking, beslutningsgrunnlag, styring og kontroll

---

SIDETALL: 83 sider, inkludert forside og vedlegg

STAVANGER, 11. Desember 2019

Forord

Takk til mine nærmeste for troen på studien min og at jeg kom i mål med masteroppgaven. En takk til gutten min som "stakk" hodet innom og spurte oppmuntrende "Hvordan går det mamma?", til mine to jenter som begge ga oppmuntrende ord underveis og bidro med å lese korrektur, og ikke minst min mann som hele veien støttet opp og oppvartet meg!

En spesiell takk til mine informanter som positivt stilte opp og ga verdigfulle opplysninger om kvalitet og behandling av risiko ved tjenesteutsetting. Dere ga alt! Deres bidrag har vært svært verdifullt og ført frem til svarene på problemstillingen.

Ønsker å gi en spesiell takk til min veileder Ole Andreas Hegland Engen for god veiledning og gode råd i arbeidet med studien. Du stilte alltid opp!

Takk også til medarbeider i Skatteetaten som tok seg tid til å se gjennom og komme med tilbakemelding på kommunikasjonsformen i intervjuguide.

En stor takk til dere alle!

Sammendrag

Tjenesteutsetting av digitale IKT tjenester ble for alvor satt på dagsorden etter flere hendelser hvor til dels store tjenesteavtaler ble trukket tilbake fra virksomheter i offentlig sektor. I flere tilfeller var bakgrunnen manglende kvalitet og for stor risiko ved avtaleinngåelsen. Det medførte at avtalene ble trukket tilbake.

Det stilles forventninger fra myndigheter til å tjenesteutsette innenfor offentlig sektor. Samtidig stilles det forventninger til at lover/forskrifter og regelverk etterleves slik at oppfylles. Kvalitet og risikostyring forventes at legges til grunn for tjenesteutsetting av digitale IKT miljøer.

Problemstilling som belyses i oppgaven er:

1) På hvilken måte vurderer offentlig sektor risiko knyttet til tjenesteutsetting av digitale IKT tjenester?
2) Hvordan innvirker disse risikovurderingene på kvaliteten av tjenesteutsettingen av digitale tjenester IKT?

med underliggende forskningsspørsmålene:

- Hvilke kritiske risikofaktorer er knyttet til risikostyringen?
- Hvilke faktorer veier tyngst i beslutningsprosesser?

Oppgaven belyser problemstillingen og besvarer med hvilken kvalitet offentlig sektor vurderer risiko, risikostyring og risikovurderinger, og hvordan det innvirker og blir håndtert ved digitale IKT tjenesteutsetting. Den belyser også hvilke kritiske risikofaktorer som er knyttet til risikovurderingene, og hvilke av disse som veier tyngst i beslutningsprosessene.

Empiri beskriver de funn som fremkom fra informantene. Metoden som er benyttet er kvalitativ metode med intervjuer. Teorien som er benyttet er hentet fra pensumlitteratur på studiet, internasjonale og norske standarder, og Temarapporter, risikorapporter og veiledninger fra myndigheter og organisasjoner.

Det avdekkes at det jevnt over er et forbedringspotensial for å oppnå god praksis og robuste tjenesteutsettinger med akseptabel kvalitet. Risikovurderinger er i varierende grad gjennomført, og med ulik kvalitet. Dette medfører at kvaliteten på risikovurderinger kan bli bedre. Mangler ved gjennomføringen av risikovurderinger påvirker beslutningsgrunnlaget som blir en kritisk risikofaktor. I beslutningsprosessene veier beslutningsgrunnlaget tyngst.

Innholdsfortegnelse

Innhold

1 Innledning

Kvalitetssikring av arbeidet som gjøres i forbindelse med anskaffelsen er vesentlig for hvor vellykket en tjenesteutsetting blir. Det er viktig at risiko og sikkerhet blir ivaretatt for tjenesten gjennom hele livsløpet. Det må legges til rette for IT investeringer som gir et trygt og bærekraftig samfunn. En robust tjenesteutsetting vil ivareta den enkelte borgers og virksomheters rettigheter.

Tjenesteutsetting er å sette tjenesten ut til en ekstern tjenesteleverandør som ivaretar oppgavene man tidligere har løst i virksomheten. Leverandøren leverer et produkt eller en tjenesten i henhold til avtalen som regulerer forholdet mellom kunden, i dette tilfelle offentlig aktør og leverandøren. Noen kaller det utkontraktering og det engelske navnet er outsourcing. Fellesbetegnelsen for alle former er sourcing. Når tjenesteutsetting skjer på tvers av landegrenser kalles det ofte offshoring på engelsk. Innenfor offentlig sektor omtales dette ofte som konkurranseutsetting. Tjenesteutsetting brukes også for å sette virksomheten bedre i stand til å ha fokus på sin kjernevirksomhet. Med tjenesteutsetting menes de ulike former som for eksempel Software as a service, Infrastructure as a service eller skytjenester. Det eksisterer i dag få skyleverandører med anlegg i Norge. *"Tjenesteutsetting ved bruk av skytjenester innebærer derfor at lagring og prosessering primært utføres på skyleverandørens anlegg utenfor Norge og dermed utenfor nasjonal kontroll."* (Stortingsmelding Meld. St. 38 2016–2017). Microsoft skal riktignok levere skytjenester fra to nye datasentre i Norge. Google har planer om å etablere datasentre for skytjenester i Norge og har kjøpt tomt til formålet.

Tjenesteutsetting vil være det begrep som benyttes videre i oppgaven.

Myndighetenes oppfordring om tjenesteutsetting (Stortingsmelding Meld. St. 38 2016–2017) og bruk av skytjenester innenfor for offentlig sektor. Det har bidratt til at offentlig sektor i større grad tjenesteutsetter IKT-tjenester. Stortingsmelding 38 sier følgende om tjenesteutsetting *"Mange virksomheter velger å anskaffe IKT-tjenester fra en eller flere eksterne leverandører i stedet for å produsere dem selv. Leveransene kan gjennomføres internt i virksomheten eller eksternt av nasjonale eller internasjonale leverandører. Det kan også være kombinasjoner av disse."* (Stortingsmelding Meld. St. 38 2016–2017)

Tjenesteutsetting av IKT-tjenester til profesjonelle aktører vil kunne gi bedre sikkerhet og mer stabile og tilgjengelige tjenester. Det kan også gi lavere og mer forutsigbare kostnader og bidra til bedre prioritering av virksomhetens kjerneområder. Dette fordrer at virksomheten

besitter kompetanse til å følge opp leverandører de setter ut tjenester til. Samtidig må virksomheten være bevisst hvilke verdier som eksponeres ved tjenesteutsetting, og iverksette nødvendige tiltak. Behovet for konfidensialitet, integritet og tilgjengelighet bør særlig vektlegges i vurderingene, og hvilke lover, krav og regler som gjelder for sektoren nasjonalt og internasjonalt.

NSM sin Temarapport Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – en utdyping av området "beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet (Nasjonal sikkerhetsmyndighet (NSM, 2018a) tar opp aktuelle problemstillinger knyttet til tjenesteutsetting.

Tjenesteutsetting av IKT tjenester stiller krav til kvalitet og risikohåndtering i arbeidet, både før, under og etter anskaffelsen. (NSM, 2018a) Det er nødvendig å ha god oversikt over kritisk infrastruktur og hva en tjenesteutsetting vil bety for det. Det er derfor behov for større aktsomhet til tjenesteutsetting av IKT tjenester i offentlig sektor. Kvaliteten på arbeidet med risikoene ved tjenesteutsetting er avgjørende for en vellykket tjenesteutsetting.

I Norge har det vært flere tilfeller av kontraktsavbrudd med bakgrunn i hendelser hvor resurser fra andre har fått urettmessig tilgang til mer enn det avtalen beskriver. I flere av tilfellene er det avdekket at det ikke foreligger eller er gjennomført svært manglende risikovurderinger. Det er avdekket manglende kvaliteten på arbeidet i forkant av beslutninger om tjenesteutsetting i anskaffelsesprosessen. Dette gjelder blandt annet Helse Sør-Øst og Digitale Gardermoen som har avsluttet sine avtaler, og det har vært belyst i media at Nødnett og Statoil (nå Eqvinor) har tatt sine tjenester tilbake. I tillegg har Statsstyrelsen i Sverige kommet i tilsvarende situasjon.

Stortingsmelding 38 IKT-sikkerhet belyser de digitale sårbarheter og oppfordrer til bevissthet og gode beslutningsgrunnlag for å redusere sårbarheter. *"I den senere tid er det utarbeidet flere analyser om digitale sårbarheter. Disse bidrar til folkeopplysning og bevisstgjøring, men også til å gi myndigheter og virksomhetsledere et beslutningsgrunnlag for å utforme politikk og tiltak for å redusere sårbarheter."* (Stortingsmelding Meld. St. 38 2016–2017).

Tjenesteutsetting av IKT tjenester og funksjoner innenfor offentlig sektor kan gi bedre økonomi og det kan gi mer forutsigbare kostnader i tjenesten. Ved bruk av profesjonelle tjenestetilbydere kan tjenestene blir mer tilgjengelige, være mer robuste og stabile, og gi bedre

sikkerhet i tjenesten. Økonomien ved tjenesteutsetting kan gi virksomheten mulighet for å rette et større fokus på etatens kjerneaktivitet. Tjenesteutsetting kan gi mange positive tilskudd til etatens tjenester. Tjenesteutsetting består av mer komplekse verdikjeder og dersom kvaliteteten i tjenesten ikke er tilstrekkelig kan det føre til mindre kontroll på tjenesten og dermed økt risiko. (Nasjonal sikkerhetsmyndighet NSM 09.04.2018) En helhetlig risikostyring vil gi det hele og fulle komplekse risikobildet ved tjenesteutsetting.
Med bakgrunn i flere hendelser, og forståelsen av tjenesteutsetting i forhold til kritisk infrastruktur og samfunnssikkerhet er behovet for studien tilstede.

Formålet med studien er å undersøke om tjenesteutsettingen er godt planlagt og gjennomarbeidet. Å identifisere om kvaliteten på forberedelsene og om kunnskapsgrunnlaget som leder frem til beslutningsgrunnlaget er tilstede og avdekket. Avklare om risikoperspektivet rundt temaene er ivaretett og om usikkerhetsmomenter er tatt hensyn til.

Studien skal identifisere hvordan kvaliteten i prosesser for tjenesteutsetting foregår innenfor offentlig sektor. Det vil undersøkes i hvilken grad kvalitet ved risikostyringen vurderes helhetlig og om det gir en bærekraftig tjenesteutsetting.

For å besvare hvordan offentlig sektor vurderer risiko ved tjenesteutsetting vil oppgaven undersøke i hvilken grad risiko identifiseres og med hvilken kvalitet det gjennomføres forberedelser og planlegging. Temaene er styring og kontroll, bestillerkompetanse, risikovurderinger, krav til IKT-tjenesten og hvem som tar beslutninger. Det vil avklares om dette gjennomføres med bakgrunn i kvalitetskrav fra god praksis i teorien, offentlige standarder og i virksomhetens egne styringssystemer. Oppgaven er bygd opp rundt disse temaene.

1.1 Problemstilling

3) På hvilken måte vurderer offentlig sektor risiko knyttet til tjenesteutsetting av digitale IKT tjenester?
4) Hvordan innvirker disse risikovurderingene på kvaliteten av tjenesteutsettingen av digitale tjenester IKT?

med underliggende forskningsspørsmålene:

- Hvilke kritiske risikofaktorer er knyttet til risikostyringen?

- Hvilke faktorer veier tyngst i beslutningsprosesser?

For å ivareta IKT-sikkerheten ved tjenesteutsetting, anbefaler Nasjonal sikkerhetsmyndighet at virksomheten er bevisst behovet for:
1 Oversikt og kontroll på hele livsløpet
2 God bestillerkompetanse
3 Gode risikovurderinger for å kunne ta riktig beslutning
4 Riktige og gode krav til IKT-tjenesten og til leverandør
5 Riktig beslutning på riktig nivå" (NSM, 2018a)

Temaene er sentrale og nødvendige for å få oversikt over risiko og oppnå god kvalitet i risikostyringen ved tjenesteutsetting. Disse vektlegges derfor i empiri, drøfting og vurdering av kvaliteten på risikostyring ved tjenesteutsettingen.
Temarapport anvendes som teori og er tatt inn oppgaven med bakgrunn i følgende:

> *"Hensikten med Temarapporten er å bistå offentlige og private virksomheter med overordnede sikkerhetsfaglige anbefalinger om hva som bør ivaretas ved tjenesteutsetting av basisdrift, applikasjonsdrift eller applikasjonsforvaltning. Anbefalingene er relevante for offentlige og private virksomheter."* (NSM, 2018a)

1.2 Avgrensning

Oppgaven dreier seg om risikostyring og ser ikke på andre forhold ved tjenesteutsetting enn kvalitet og risiko. Oppgaven vil således omtales kun i forhold til kvalitetsaspektet. Økonomi, og Helse, Miljø og Sikkerhet funksjoner i et globalt, nasjonalt eller organisatorisk perspektiv er ikke en del av denne oppgaven.

2 Teori

For å besvare problemstilling er det valgt teori knyttet til kvalitet og risiko da problemstillingen søker besvart risiko knyttet til risikofaktorer ved tjenesteutsetting og hvordan kvaliteten av disse vil påvirke risikostyringen. I tillegg er knyttet teori direkte opp mot oppgavens inndeling i de ulike temaene. Dette understrekes spesielt i NSM sin Temarapport *"Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – en utdyping av området "beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet"*. (NSM, 2018a). Teorikapittelet vil derfor ha fokus på ulike verktøy som standarder og rammeverk for styringssystemer for kvalitets-, risiko- og ledelsessystem. Herunder vil det være fokus på leverandørstyring og risikovurdering, kvalitet, risiko, og sikkerhet.

2.1 Teoribegrep og definisjoner

Det er mange likheter og stort sett ingen motsetninger i bruk av begrep og definisjoner mellom de ulike rammeverk, veiledere og ISO-standardene for kvalitet og benyttede risikobegrep. De har likevel en noe ulik tilnærming, vektlegging og begrepsbruk. På bakgrunn av disse forskjellene vil det variere hvilke rammeverk og standarder som benyttes som utgangspunkt for definisjon og forståelse av begrep ut fra hvilke tema, perspektiv, begrep og vektlegging som brukes til enhver tid.

I det følgende presenteres oppgavens teoretiske rammeverk. I oppgaven anvendes de ulike begrep for å bestemme hvordan kvalitet og risiko blir vurdert i forhold til tjenesteutsetting i offentlig sektor.

Disse begrep legger rammeverk for de begrepene jeg legger til grunn i oppgaven. Jeg vil derfor i det påfølgende definere de sentrale begrepene kvalitet og risiko med tilhørende begrep innen tema Styring og kontroll inkludert leverandørstyring, Risikovurdering, Bestillerkompetanse, IKT-tjeneste, Beslutningsledelse. Disse er viktige i denne sammenhengen fordi de er sentrale begreper ved kvalitet og risiko knyttet til tjenesteutsetting og vil påvirke resultatet av den.

Rammeverk, standarder og veiledninger er alle verktøy og hjelpemiddel som skal legge til rette for, og bidra til, styring av risiko, internkontroll og god kvalitet i virksomhetens produkt- og tjenesteleveranser. Bruk og etterlevelse av disse må ikke bli et mål i seg selv, de skal

understøtte god styring og kontroll og således bidra til måloppnåelse. Hvilke standarder, rammeverk og veieldninger som benyttes vil variere utfra hva som er mest hensiktsmessig å støtte seg på i oppgaven for å definere benyttede begrep for å kunne oppfylle krav og måloppfyllelse og ved noen anledninger å kombinere flere. Dette er under forutsetning av, og så fremt det ikke er fastsatt i lov eller forskrift, eventuelt fra overordnet departement, at spesifikke standarder eller rammeverk skal følges eller legges spesielt til grunn ved tjenesteutsetting.

2.2 Kvalitetsbegreper og modeller

Kvalitet på hvordan styring av risiko står sentralt i oppgaven. Problemstillingen er knyttet opp mot dette på følgende måte "På hvilken måte vurderer offentlig sektor risiko knyttet til tjenesteutsetting av digitale IKT tjenester?" og "Hvordan innvirker disse risikovurderingene på kvaliteten av tjenesteutsettingen av digitale tjenester IKT?" Det vil således være avgjørende i oppgaven å finne svar på hva offentlige etater legger ned av arbeid i forhold til å få en god kvalitet på arbeidet med risiko ved tjenesteutsetting. Dette er relevant både før, under og etter tjenesteutsetting. Kapittelet tar for seg de teoretiske perspektiver på kvalitet, både definisjoner og kvalitetsstandarder.

Sentralt i standarden for kvalitet står prosesstankegangen og kundeperspektivet. Kvalitetsarbeid handler mye om kvalitet i gjennomføringen av prosesser og kvalitet med tilhørende produkter og tjenester (eksempelvis interne kvalitetskrav, krav fra kunder og eksterne (lover og regler), og oppmerksomheten på brukere (kunder) (NS-EN ISO 9001:2015).
Dette er også forenelige med to av tre målsettingskategorier, som står sentralt i COSOs internkontrollrammeverk, nemlig målrettet og effektiv drift og overholdelse av lover og regler (COSO ERM, 2017).
Disse beskrivelsene ligger også til grunn i kvalitetsbeskrivelsene fra DFØ hvor Internkontroll-metode baserer seg på COSO med inspirasjon fra ISO-9001:2008 standarden. (NS-EN ISO 9001:2008)

Utfra problemstillingen vil kvaliteten måles på aktuelle begreper temaene fra Temarapport (NSM, 2018a), bærekraft ved tjenesteutsetting, helhetlig risikostyring (Enterprise Risk Management ERM), modenhet og samfunnssikkerhet være sentrale.

En velkjent definisjon av Kvalitet er fra NS-EN ISO 9001:2015 som sier *"i hvilken grad en samling av iboende egenskaper oppfyller behov eller forventning som er angitt, vanligvis underforstått eller obligatorisk"*. Flere tar utgangspunkt i NS-EN ISO 9001:2015 da de etablerer rammeverk og styringssystem for Kvalitet og Direktoratet for økonomiforvaltning, (heretter betegnes som DFØ) er en av aktørene som har benyttet seg av det og lagt denne til grunn i sin formulering av beskrivelse av kvalitet. DFØs metode baserer seg riktignok på COSO med inspirasjon fra ISO.

En annen velkjent beskrivelse for statlig sektor av behovet for kvalitetsstyring er Direktoratet for økonomiforvaltning sin beskrivelse i veileder for internkontroll *"Det å innføre et system for kvalitetsstyring i tråd med ISO er en strategisk beslutning som ledelsen i virksomheten bør ta på lik linje med valg av hvilke standarder eller rammeverk virksomheten skal støtte seg til for å oppnå god styring og kontroll."*. Den sier videre *"Alle rammeverk og standarder endrer seg over tid. Også ISO-standardene er i endring. De som gjelder styring og kontroll blir harmonisert for å forenkle samordning og helhetlige styringssystem i praksis"*. (dfo.no) Flere offentlige etater og sektorer benytter rammeverk og styringssystemer fra DFØ og definisjoner og beskrivelser herfra anses derfor relevant da oppgaven omhandler offentlig sektor. På virksomhetsnivå handler det altså om hvordan produkt eller tjeneste tilfredsstiller kundens krav. (dfo.no)

Store norske leksikon definerer Kvalitet som *"er tings måte å være på, tingens beskaffenhet. Når ordet kvalitet brukes om sanseinntrykk, betyr det spesifikk karakter. For en gjenstand eller tjeneste kan man enkelt si at kvalitet er evnen til å tilfredsstille brukerens krav og forventninger"*. (kvalitet – Store norske leksikon *https://snl.no/kvalitet)*

Definisjon av kvalitet har uavhengig av kilde mange likheter og små variasjoner i beskrivelsene. I oppgaven vil jeg forstå kvalitet som at man gjør en grundig dybdevurdering og faglig godt fundert vurdering av egenskapene til kvalitet. Det betyr for meg en identifisering og kartlegging av kvalitet på alle viktige og riktige forhold knyttet til tjenesteutsetting med utgangspunkt i temaene i Temarapport (NSM, 2018a). Slik vil man best oppnå styring av risiko og god kvalitet på tjenesteutsettingen.

Med bakgrunn i at problemstillingen knytter seg til offentlig sektor vil beskrivelsen til DFØ legges til grunn når kvalitet diskuteres. Dette med bakgrunn i at DFØ benyttes av statlig sektor hvor flere følger deres veiledninger. I oppgaven er det hensiktsmessig å legge vekt på kvalitet på de tema som drøftes og vurderes fra Temarapport (NSM, 2018a). Når man forstår begrepet kvalitet i dimensjonen av å gi robusthet, vil det oppnås forutsigbarhet i tjenesteutsettingen.

2.2.1 Modenhet

Det er mange forhold som påvirker kvalitet og risiko ved tjenesteutsetting. Hvor stor modenhet det offentlige har om viktigheten av styring på risiko og kvalitet i arbeidet ved tjenesteutsetting vil være avgjørende for hvor stor oppmerksomhet risiko får og hvilken kvalitet som ligger i arbeidet med tjenesteutsetting. For å oppnå god kvalitet på styringen av risiko er modenhet et viktig moment. Dersom offentlig sektor ikke er modne nok vil det påvirke styringen og kontrollen på risikoen. Myndighetene har økt fokus på håndtering av risiko gjennom reguleringsregime. Her er det fokus på hva det stilles krav til og det blir gitt føringer til dels gjennom lov og forskrifter, men også gjennom ulike utredninger (NOU 2018:14) og dokumenter (St.mld. 38, 2017). Ved hjelp av dette modnes offentlig sektor sakte, men sikkert. Det er likevel slik at modenhetsnivået vil måtte måles for å finne hvilket nivå de ulike etater og sektorer er på. Til hjelp kan ulike rapporter for måling av modenhetsnivå benyttes. I denne oppgaven er det valgt å vektlegge dette ved tjenesteutsetting. (Sæther, Hans Solli 2016)

Modenhetsnivå for tjenesteutsetting vil kunne settes ut fra nedenstående tabell for rammeverk for anlayse av modenhetsnivå. (Sæther, Hans Solli 2016)

Rammeverk for analyse av modenhetsnivå.

NivåRefe-ransemål	Intern funksjon	Intern servicefunksjon	Outsourcing	Offshoring	Backsourcing
Kostnader	Kostnads-bekymringer	Etablering av basislinje for servicenivå og kostnader	Høyere produksjons-kostnader enn forventet	Uforutsette transaksjons-kostnader	Kostnads-minimering og operasjonell effektivitet
Ressurser	Tilgang til dyktige ressurser	Profesjonalisering av servicefunksjonen	Tap av kontroll over ressurser og servicefunksjoner	Kunnskapsgap mellom kunde og leverandør	Tilgjengelighet av interne ressurser
Partnerskap	Problemer i forholdet mellom funksjon og linjen	Dokumenterte avtaler mellom servicefunksjon og linjen	Kontraktsforhold mellom klient og leverandør	Forskjeller mellom partene når det gjelder geografi, tidssoner, språk og kulturer	

Tabell 1: Rammeverk for analyse av modenhetsnivå, Modenhet i outsourcing, offshoring og backsourcing: Tilbake til fremtiden? Kilde: Sæther, Hans Solli 2016

Rammeverket for analyse av modenhet illustreres i tabell 2 ved hjelp av eksempler fra norsk næringsliv. Tre bedrifter er valgt og beskrevet slik at de viser stegvis utvikling og dominerende problemer for hvert nivå. Nærstudier i bedriftene er utført av forskeren selv eller i samarbeid med andre forskere. (Sæther, H. S., 2016)

Anvendelsen av modenhetsmodellen for outsourcing, offshoring og backsourcing har lært oss at beslutning om sourcing initierer omfattende organisatoriske endringsprosesser. Beste praksis viser at norske bedrifter: 1) har høyt fokus på produktivitet, automatisering og nye produksjonsformer, 2) utvikler og integrerer ressurser og kompetanse som understøtter den strategiske kjernen, og 3) legger vekt på utvikling av partnerskapet. På denne måten kan endringsprosessen bidra til å gi bedriften økt konkurransekraft.

For bedriftsledere representerer modenhetsmodellen et bilde av utviklingen, der bedriftens modenhetsnivå kan forstås både i form av historien og fremtiden. Bedrifter kan bruke modellen til å identifisere på hvilket nivå de befinner seg. Den kan hjelpe ledere til å identifisere kommende utfordringer, og dermed gi en ramme for fremtidig planlegging og utvikling. Områder for benchmarking kan indikere problemområder som fortjener spesiell oppmerksomhet.

For forskere kan modenhetsmodeller ha potensial til å skape ny kunnskap og innsikt i organisatoriske fenomener. Slike modeller representerer verktøy for teoribygging som konseptualiserer utvikling over tid. Denne modenhetsmodellen for outsourcing, offshoring og backsourcing representerer en teori som kan bli utforsket og empirisk validert. (Sæther, Hans Solli 2016)

Forståelsen av modenhet i denne sammenhengen er om virksomhetene viser om deres tilnærming til tjenesteutsetting følger de føringer som beskrives i rammeverk om modenhet.

2.3 Risikobegrep og modeller

Risiko handler om flere forhold, det gir et mulighetsrom på den ene siden og behov for sikring på den andre siden. Risikoaspektet handler om kunne ta, og når det kan tas risiko. Å avbalansere disse to er viktig for å finne balansen på hvilken risiko man er villig til å ta for å oppnå et akseptabelt risikonivå.

2.3.1 Risiko

Risiko opptrer i mange dimensjoner; hva er det konkrete risikoelementet, hva gjør man for å styre risikoen, hvordan vurderer man den, og hvor finner man risikoaksepten. Teorikapittelet tar for seg de ulike perspektivene ved risiko og relateres til disse gjennom hva som er "god praksis" ved risikostyring, - vurdering, -aksept og -behandling. Disse risikoelementene, som del av "god praksis", er nødvendig og bør være vurdert og håndtert for å oppnå kontroll på risiko ved tjenesteutsetting. Det teoretiske aspektet ved disse beskrives senere i teorikapittelet.

Risiko, og kvalitet på hvordan det jobbes med ved tjenesteutsetting, er essensen i oppgaven. Problemstillingen reflekterer dette på følgende måte "På hvilken måte vurderer offentlig sektor risiko knyttet til tjenesteutsetting av digitale IKT tjenester?", og "Hvordan innvirker disse risikovurderingene på kvaliteten av tjenesteutsettingen av digitale tjenester IKT?". Med bakgrunn i problemstillingen, vil de teoretiske perspektivene for risiko ta for seg alle dimensjoner av hva risiko kan bety.

De ulike definisjonene av risiko har som nevnt tidligere mange likhetstrekk, samt enkelte ulikheter knyttet til hva de skal brukes til. Risiko defineres og beskrives på ulike måter og i enkelte tilfeller avhengig av om det er basert på forventningsverdier og økonomiske faktorer, eller basert på sikkerhet og enkelte økonomiske sammenhenger (Aven T., 2015). Definisjon av risiko har likevel, uavhengig av kilde mange likheter og små variasjoner i beskrivelsene.

Aven påpeker at "begrepet risiko ikke er helt klart" da det finnes flere definisjoner avhengig av formålet. Han definerer risiko i sammenhengen opp mot oppgaven som *"kombinasjon av konsekvenser C av aktiviteten og tilhørende usikkerhet U (vi vet ikke hva C vil bli)"* (Aven 2015).

Engen m fl. beskriver flere former for risiko ved ulike vurderingskriterier og risikobeskrivelser. De ser på risikobegrepet som et kunnskapselement. Måten Engen m fl. definerer risiko på er *"Sannsynlighet x Konsekvens"* (Engen mfl. 2016).

En annen måte å definere risiko på refererer til usikkerhet om alvorligheten av hendelser og konsekvenser (eller resultater) av en aktivitet med hensyn til noe mennesker verdsetter (Aven & Renn 2010)

En velkjent definisjon av risiko er fra NS-ISO 31000, som beskriver risiko som *"virkning av usikkerhet knyttet til mål"* [SN-ISO Guide 73:2009, definisjon 1.1].

En annen kjent definisjon av risiko for offentlige virksomheter er Direktoratet for IKT og forvaltning (Difi) sin som sier "*Risiko handler om potensielle avvik fra det forventede eller potensielle avvik fra våre mål. Med det referansepunktet defineres risiko formelt som en kombinasjon av mulige konsekvenser (utfall eller resultat) og tilhørende usikkerhet."* (Difi, 2019)

Usikkerhet kvantifiseres ved hjelp av sannsynligheter. Vi benytter derfor ofte en variant av definisjonen foran og sier at risiko er kombinasjonen av (mulige) konsekvenser og (tilhørende) sannsynligheter, eller bare at risiko er kombinasjonen av konsekvens og sannsynlighet.

En annen velkjent beskrivelse av risiko for statlig sektor er DFØ sin, som omtaler risiko som *"Forhold eller hendelser som inntreffer og påvirker måloppnåelsen kan ha negative konsekvenser, positive konsekvenser eller begge deler".* DFØ kaller forhold eller hendelser som kan inntreffe og påvirke måloppnåelsen negativt, for risiko. Hendelser med positive konsekvenser representerer muligheter. Begge deler er like viktig å fokusere på for ledelsen. (DFØ, 2019)

Med begrepet risiko forstår jeg det som at det kan beskrives som forhold eller hendelser som kan inntreffe og påvirke oppnåelse av målsettinger negativt. Denne definisjonen bygger på DFØ sin beskrivelse og forståelse av risiko. I denne oppgaven er det derfor hensiktsmessig å legge vekt på muligheten for styring og måloppnåelse ved tjenesteutsetting når man forstår begrepet risiko.

2.3.2 Risikoregulering

Risikoregulering består gjerne av flere elementer og beskrives i teori på litt ulike måter i ulike teorier.

I Baldwin og Cave beskrives regulering med "Regulation is a topic that stimulated interest in a host of disciplines - notably low, economics, political science, sociology, history, psychology, geography, management and social administration" (Baldwin og Cave 1999), og Baldwin mfl. 2012 beskriver risikoregulering med tre hovedtemaer (Baldwin mfl. 2012). Engen mfl. beskrives seks temaer for risikoregulering rundt seks temaer knyttet til risikoregulering; grunnleggende juridiske begreper og retningslinjer om juridisk metode, begrepet "reguleringsregime", samstyring som omfatter horisontale og vertikale mekanismer

for styring og kontroll innenfor organisatoriske og institusjonelle rammer, normer for adferd og internkontroll (Engen mfl. 2016).

Røyksund beskriver en oversettelse av Balwin og Cave som spesifikke regler ("set og commands"), tilsiktet statlig påvirkning og alle former for sosial og økonomisk påvirkning (Røyksund Mai 2018) (Baldwin og Cave 1999).

I Baldwin mfl. beskrives det som presise regler, lover vedtas av Stortinget, forskrifter av forvaltning, forordninger og direktiver EØS, samfunnskontroll som pålegg fra Staten eller lokalsamfunn/sivilsamfunn eller tredjepart som utsettes for farer eller risiko, og tvungen statlig påvirkning som skattelegging og avgifter og også økende for å fremme miljøvennlig produksjon og bærekraftig økonomisk aktivitet (Baldwin mfl. 2012).

Risikoregulering mot offentlig sektor for risiko skjer gjennom myndighetenes føringer og pålegg. Flere myndighetsaktører som NSM, PST, E-tjenesten og DSB lager årlige risikorapporter. Både Stortingsmeldinger, Norges offentlige utredninger (NOU), strategier og Temarapporter gir føringer for anvendelse. I denne oppgaven vil Engen mfl. sin forståelse av risikoregulering legges til grunn i drøfting.

2.3.3 Risikofaktorer

Risikofaktorer er en av perspektivene i problemstillingen. Det finnes flere innfallsvinkler tilhva en risikofaktor og dens betydning. Hood mfl. sin beskrivelse av risikofaktorer er et større, overodnet omfang. De beskriver det som økonomiske forhold, helse/arbeidsmiljø, teknisk og ytre miljø, som offentlighet/oponion som formidling, fortolkning, politisk interesse og debatt, eller som interessenter som industri, fagforeninger, media, aksjonsgrupper (Hood mfl. 2001).

NSM Risiko 2019 tar for seg 6 risikofaktorer. De tar for seg et ufullstendig risikobilde, svak sikkerhtsstyring, mangler i virksomhetens personellsikkerhetsarbeide, utilstrekkelig sikring av samfunnsviktig informasjon og informasjonssystemer, for få utpekte skjermingsverdige objekter og infrastrukturer, og næringslivets levering av tjenester og utstyr av samfunnsfunksjoner sett opp mot at det vurdres og dimesjoneres risikoreduserende tiltak med dette som bakteppe (NSM, 2019 a). Disse seks med unntak av skjermingsverdige objekter og infrastruktur i sammenheng med oppgavens problemstilling er alle aktuelle risikofaktorer som vil belyses i drøfting i oppgaven.

I denne oppgaven vil jeg utfra problemstilling og dens betydning av risikofaktorer forstå risikofaktorer i betydningen av hvordan NSM beskriver disse i sin risikorapport (NSM, 2019 a).

2.3.4 Risikostyring

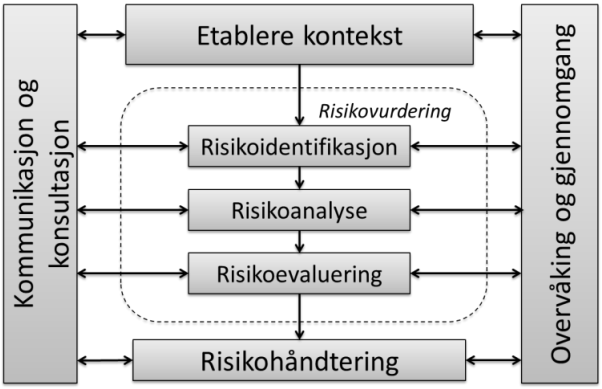
Risikostyring er viktig for å oppnå balanse i sammenhengen mellom risiko og gevinst. Det er prosessen for å oppnå kort- og langsiktig balanse mellom disse. Dette må sees i sammenheng med hver enkelt virksomhets ønskede risikoeksponering. I oppgaven vil risikostyring benyttes for å vurdere om det er god kvalitet i arbeidet med å styre risiko. Det er benyttet flere definisjoner av begrep og modeller for risikostyring i oppgaven. Noen av disse er komplementære, andre er overlappende.

Aven definerer risikostyring på følgende måte: *"med risikostyring forstås alle de tiltak og aktiviteter som gjøres for å styre risiko"*(Aven T., 2015). Aven påpeker spesielt behovet for et rammeverk for riskostyring (Aven T., 2015)

NS-ISO 31000:2009 standarden definerer risikostyring som *"koordinere aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko (2.1)"* [SN-ISO Guide 73:2009, definisjon 2.1] Den har som formål å *"hjelpe virksomheter å øke graden av måloppnåelse, bedre identifikasjon av muligheter og trusler, og effektivt allokere og bruke ressurser for risikohåndtering. Det forutsettes også at et helhetlig perspektiv på tvers av organisasjonsenheter, funksjoner og risikokategorier (strategiske, finansielle, operasjonelle risikoer mv.) legges til grunn, for å unngå silotenking og suboptimalisering"*. (Standard Norge, 2019)

En forutsetning for å lykkes er at ledelsen:

- Etablerer og eier risikostyringspolitikken
- Sikrer samsvar mellom organisasjonskultur og risikostyringspolitikk
- Fastsetter risikostyringsmål i samsvar med organisasjonens mål og strategier
- Sikrer nødvendige ressurser, samt hensiktsmessighet til rammeverk
- Sikrer eierskap i organisasjonen:



FIGUR 1 RISIKOSTYRINGSPROSESSEN KILDE NS-EN ISO 31000:2009

- Tildeler ansvar
- Kommuniserer fordeler ved risikostyringsarbeidet

Figur 2: Risikostyring, kilde Standard Norge

DFØ definerer risikostyring i Staten som *"Risikostyring er et viktig hjelpemiddel i styringen. Risikostyring består av to hoveddeler:*

1. *Risikovurderinger (risikoidentifikasjon, risikoanalyse og risikoevaluering/prioritering)*
2. *Risikohåndtering (utforming av risikoreduserende tiltak og oppfølging av risiko)*

Resultatet av vurderingene angir hvor høy den enkelte risiko er." (DFØ, 2019d).

Direktoratet for IKT og forvaltning (Difi) beskriver riskostyring slik *"Risikostyring er et sett av aktiviteter for å styre og kontrollere risiko. De kalles ofte «risikostyringsprosessen», men aktivitetene er ikke nødvendigvis sekvensielle. De ulike aktivitetene kan i hovedsak være foranlediget av hvilken som helst av de andre aktivitetene"*. De henviser videre til *"de meste anerkjente referansene er rammerverket COSO ERM og standarden ISO 31000"*. (Difi, 2019).

IIA/COSO ERM Norge sin veileder for risikostyringsfunksjonen har operasjonalisert flere rammeverk og standarder og laget "beste praksis" for risikostyringsfunksjonen. Denne er relevant for å vurdere helhetlig risikostyring og konsekvensene for virksomheten. (IIA Norge, 2017). De beskriver risikostyring i sin veileder for risikostyringsfunksjon som *"systematiske, koordinerte og proaktive aktiviteter som er rettet mot vurdering og håndtering av usikkerhet og hendelser som kan påvirke måloppnåelsen"* (IIA Norge, 2017).

Med risikostyring forstår jeg koordinerte aktiviteter for å styre og kontrollere mot målet til virksomhetene, med hensyn til risiko. Det vil gi god styring og kontroll på aktiviteter, prosesser og de tiltak som til sammen tarned risikobildet. Denne definisjonen bygger på definisjoner og begreper fra blant annet Direktoratet for IKT og forvaltning, Aven og ISO 31000. De øvrige definisjoner oppfattes mer i retning av selve prosessen for gjennomføringen av prosessen for risikostyring.

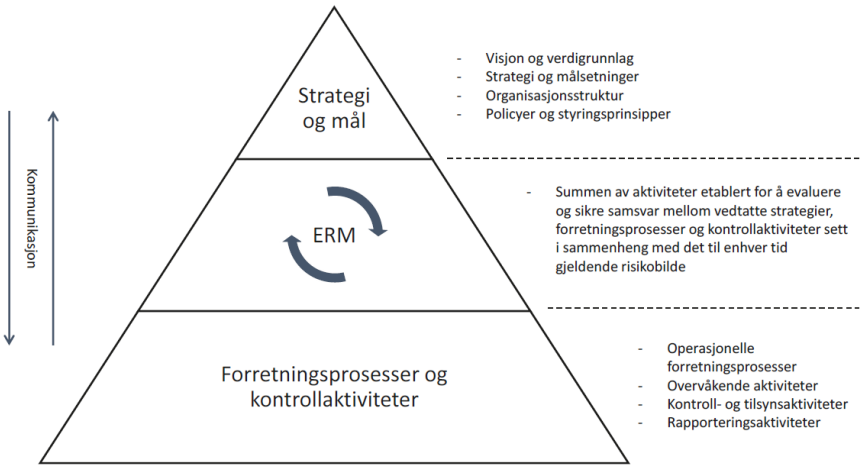
På bakgrunn av at oppgaven tar for seg tjenesteutsetting i offentlig sektor vil jeg i det videre ta med meg definisjonen til DFØ (DFØ, 2019d) og IIA Norge (IIA Norge, 2017) i risikostyringen da den første representerer statlig sektor og den andre representerer kommunal sektor. Det vil imidlertid bli henvisst til flere at modellene for risikostyring som er beskrevet i denne teoridelen.

2.3.5 Helhetlig risikostyring (Enterprise Risk Management (ERM)

Enterprise Risk Management (ERM) er en helhetlig måte for risikostyring og benyttes for å oppnå målstyring og tar i bruk metoder og prosesser til å håndtere det. Helhetlig risikostyring kan også sees på som risikobasert tilnærming. De ulike risikoområdene ivaretas gjennom dette. Disse ulike risikoområdene vil kunne være tildels komplekse forhold og vil ivareta risikostyringsprosesser.

Helhetlig risikostyring defineres av COSO (s.d.) som "Helhetlig risikostyring er en prosess, gjennomført av virksomhetens styre, ledelse og ansatte, anvendt i fastsettelse av strategi og på tvers av virksomheten, utformet for å identifisere potensielle hendelser som kan påvirke virksomheten og for å håndtere risiko slik at den er i samsvar med virksomhetens risikoappetitt, for å gi rimelig grad av sikkerhet for virksomhetenes måloppnåelse." (COSO ERM, 2017)

Enterprise Risk Management (ERM) rolle i virksomhetsstyring:



Figur 3: Forholdet mellom ERM og virksomhetsstyring kilde IIA Norge 2017

Med begrepet helhetlig risikostyring forstår jeg den helhetlige tilnærmingen til å få med alle risikoelementer og se disse i sammenheng. Med den tilnærmingen vil det gi en god oversikt og et helhetsbilde å styre etter.

2.3.6 Risikovurdering

Som en del av den totale risikohåndteringsprosessen er risikovurdering et viktig og nødvendig for håndtering av risiko. Ikke minst er en forståelse av trusselbildet vesentlig. Ved gjennomføring av risikovurdering vil bevissthet om kunnskapsgrunnlaget og usikkerhet også spille en avgjørende rolle. Det danner grunnlaget for videre vurdering av akseptabelt risikonivå. Risikohåndtering er en kontinuerlig prosess for å sikre virksomhetens verdier. Ulike vurderinger og beslutninger må fattes underveis i risikohåndteringsprosessen (Engen mfl., 2016).

Det finnes mange definisjoner på risikovurdering. Flere av disse er overlappende, andre avviker fra hverandre avhengig av hvilket område som skal risikovurderes.

Standard Norge beskriver risikovurdering som *"Risikovurdering er en samlet prosess som består av planlegging, risikoanalyse og risikoevaluering. Dette handler om å identifisere farer og uønskede hendelser, analysere og evaluere risiko, og identifisere tiltak som kan redusere risikoen"* (Standard Norge, 2019).

En velkjent definisjon av risikovurdering er NS-ISO 31000:2009 sin som beskriver det som *"samlet prosess som består av risikoidentifisering (2.15), risikoanalyse (2.21) og risikoevaluering"* (2.24) [SN-ISO Guide 73:2009, definisjon 3.4.1].

En annen offentlig aktør som har beskrevet risikovurdering er Direktoratet for IKT og forvaltning. De har beskrevet begrepet som *"Risikovurdering er et begrep i risikostyringen som dekker de tre stegene risikoidentifisering, risikoanalyse og risikoevaluering"* (Difi, 2019). Dette er en begrepsbruk som er forankret i den internasjonale standarden NS-ISO 31000 «Risikostyring». NS-ISO/IEC 27001:2017, som dette veiledningsmateriellet baserer seg på, bygger på og refererer til denne overordnede risikostyringsstandarden.

Begrepet risikovurdering forstår jeg som i henhold til en samlet prosess som består av risikoidentifisering, risikoanalyse og risikoevaluering av et risikovurderingsobjekt og som beskriver risikoelementene. Denne forståelsen bygger på artikler ISO 31000 (NS-EN ISO 31000:2009). I denne oppgaven er det derfor hensiktsmessig å legge vekt på om det forefinnes rammeverk, metoder for prosessen, og om det gjennomføres risikovurderinger og med hvilken kvalitet i forkant av tjeneutsetting.

2.3.7 Risikohåndtering, behandling og aksept

Risikohåndtering er en prosess for å velge og iverksette tiltak som skal redusere risiko. Behandlingen skal foregå på riktig nivå og med nødvendig kunnskapsgrunnlag for å kunne fatte en beslutning (Aven, 2015). Dette er en forutsetning for å kunne få frem risikoakseptkriterier og beslutningskriterier for å gi et akseptabelt risikonivå (Aven, 2015). Risikoaksept eller som noen beskriver det som risikoapetitt baseres på en besluttet plan for risikohåndtering av de viktigste risikopunktene fra risikovurderingen.

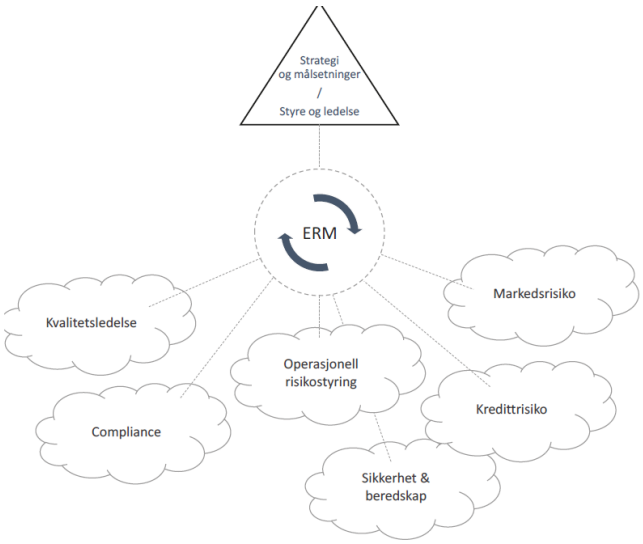
2.4 Kvalitet på risiko ved tjenesteutsetting i offentlig sektor

Teorikapittelet er i det videre bygd opp etter temaene i Temarapport (NSM, 2018a) med styring og kontroll, bestillerkompetanse, risikovurdering, krav til IKT-tjenesten og beslutningsteori. Dette understrekes ikke minst i NSM sin Temarapport *"Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – en utdyping av området "beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet"* (NSM, 2018a). For tema Styring og kontroll er perspektiet som legges her utvidet til å gjelde styringsdimensjonen i forhold til hva og hvilke styringssystemer som etablert, og hvilke prosesser som legges til grunn ved tjenesteutsetting. Dette vil bidra til å avdekke hvilke faktorer som vil påvirke kvaliteten på risiko.

2.4.1 Styring og kontroll

Styring og kontroll forstår jeg som alle de aktiviteter hvor risikostyringen bidrar til å få styring på, og slik oppnå, kontroll på tjenesteutsettingen. Denne definisjonen bygger på

helheten i de aktiviteter som gjennomføres for å oppnå styring og kontroll. Videre oppnår man en helhetlig styring og kontroll som gir bærekraftig utvikling av tjenesteutsettingen. I denne sammenhengen er derfor hensiktsmessig å legge vekt på om det er etablert prosesser for styring. Slik begrepet forstås her er det å koble den helhetlige risikostyringen til strategi og målsettinger, slik at ledelse og styre får reell mulighet til å styre risiko, oppnå god kvalitet i risikostyringen og derigjennom sette akseptabelt risikonivå. Nedenfor er en skisse som beskriver den helhetlige risikostyringen gjennom koordinering og styring av ulike risikoområder.



FIGUR 4: EKSEMPEL PÅ ERM KOORDINERING OG STYRING AV ULIKE RISIKOOMRÅDER KILDE IIA NORGE 2017

Det er flere aktuelle rammeverk for oppbygging av risikostyringsarbeidet i virksomheten hvor de mest anerkjente er ISO 31000:9000 Risk Management og COSO:2004 Enterprise Risk Management. ISO 31000 Risk Management beskriver forholdet mellom prinsipper som skaper verdier, rammeverket som gir føringer og prosessen for risikostyringen. (Norsk standard NS-ISO 31000:2009). COSO:2004 Enterprise Risk Management beskriver forholdet mellom risikostyringen og internkontrollen, og bygger på prinsippene i rammeverket for internkontroll (COSO:2004) (IIA Norge2017).

En annen velkjent standard som tar opp i seg også risikovurdering er NS-ISO 27001(NS-ISO/IEC 27001:2013). Denne standarden er aktuell i denne sammenheng da flere offentlige etater benytter denne standarden til å bygge styringssystem for informasjonssikkerhet. Denne er således aktuell da oppgaven er innenfor det digitale/IT og mange offentlige sektorer

benytter denne til å regulere sikkerhetsstyringen og således også risikostyringen. Difi sin metode for interkontroll/styringssystem bygger også på denne standarden (Difi, 2019).

Nasjonal sikkerhetsmyndighet sin Temarapport for tjenesteutsetting tar opp styringspremissene som må ligge til grunn for risikostyring ved tjenesteutsetting. Temarapporten fokuserer på temaene oversikt og kontroll på hele livsløpet, god bestillerkompetanse, gode risikovurderinger for å kunne ta riktig beslutning, riktige og gode krav til IKT-tjenesten og leverandør, og riktig beslutning på riktig nivå. (NSM, 2018a)

Det er derfor hensiktsmessig å legge vekt på at risikostyringen bidrar til en helhetlig prosess for god kvalitet på temaene fra NSM Temarapport (NSM, 2018a). Studien bygger på hvordan risikostyring ivaretar dette for virksomhetene ved tjenesteutsetting. Det vil bidra til økt fokus og forståelse av kvaliteten på tjenesteutsettingen. Temarapporten til Nasjonal sikkerhetsmyndighet har som mål å heve kvaliteten på risikostyringen ved tjenesteutsetting (NSM, 2018a).

Et annet viktig forhold i risikostyring er landvurderinger. Det er satt mer fokus på hva det betyr dersom landrisikoen blir for høy på blandt annet daktoer som korrupsjon, spionasje og sabotasje fra andre lands statlige etterretning, og knytning mellom leverandør og statlig etterretning. NSM sin Temarapport for anbefaling om landvurderinger ved tjenesteutsetting tar opp hvordan man bør håndtere dette (NSM, 2018b).

Dette er rammeverk som legges til grunn for risikostyringen og kvalitetsstyring i arbeidet med det i virksomheter. Noen virksomheter, men ikke alle, har etablert rammeverk for risikostyring. Det gir gode føringer for styring og god kontroll ved å implementere et rammeverk for risikostyring i virksomheten.

Ved tjenesteutsetting vil disse standardene kunne anvendes for å få styring og kontroll. Følges disse føringene vil det gi god kvalitet på risikostyringen.

2.4.2 Bestillerkompetanse

For å kunne få kartlagt og identifisert behovet for tjenesteutsetting, hvilken form det skal ha og få de korrekte kravene til IKT-tjenesten og IKT-sikkerhet er det nødvendig å benytte seg av tverrfaglig kompetanse slik at alle områdene for fagkompentanse blir dekket (NSM, 2018a). Dette vil gi det nødvendige kunnskapsinnhenting og forståelse som igjen vil gi et

robust og godt besluningsgrunnlag. NSM Temarapport som beslyser hvilken bestillerkompetanse ressurser som bør involveres og hvor det anbefalinges at man "ivaretar behovet for bestillerkompetanse gjennom hele
livsløpet til tjenesteutsettingen, og som et minimum har følgende kompetanseområder ved en tjenesteutsetting er virksomhets-, sikkerhets-, integrasjons-, anskaffelse- og juridisk kompetanse som blir benyttet ved tjenesteutsetting, og innehar disse funksjonene nødvendig grunnleggende IKT kompetanse" (NSM, 2018a). Denne totale bestillerkompetansen er det ingen av virksomhetene som har innehatt, men en av virksomhetene har etablert det i etterkant av en uheldig tjenesteutsetting.

Engen mfl. "snakker om de egeneskapende deltakende aktører må besitte for å bidra med innflyttelse (Engen mfl., 2016). Videre presisserer Engen mfl. at "Jo mer en aktør har av innflyttelsesressurser, jo større muligheter har han til å kunne påvirke beslutningsprosessen og resultatet." (Engen mfl., 2016 s. 178).

2.4.3 Risikovurdering

I dette avsnittet skal jeg redegjøre for hvordan risikovurdering tolkes og anvendelsen innenav det i denne oppgaven. Som nevnt ovenfor er risikvurderinger nødvendig for å oppnå kvalitet på risiko og bør bestå av systematiske og planlagte prosesser (NS-EN ISO 31000:2009) (Aven T., 2015).

En velkjent metode er risikovurdering etter ISO standard sin risikostyringsprosess. Direktoratet for IKT og forvaltning (Difi) henviser også til denne og benytter beskrivesen *"Risikovurdering er et begrep i risikostyringen som dekker de tre stegene risikoidentifisering, risikoanalyse og risikoevaluering"*. Dette er en begrepsbruk som er forankret i den internasjonale standarden NS-ISO 31000 «Risikostyring». NS-ISO/IEC 27001:2017, som dette veiledningsmateriellet baserer seg på, bygger på og refererer til denne overordnede risikostyringsstandarden (NS-EN ISO 31000:2009).

Denne er således aktuell da oppgaven er innenfor det digitale/IT og mange offentlige sektorer benytter denne til å regulere sikkerhtsstyringen og gjennom det belyse og styre hvordan risikovurdering skal foregå. Risikovurderingsprosessen fra standardens risikostyringsprosess brukes av flere offentlige sektorer til å gjennomføre risikovurderinger.

I denne oppgaven er derfor hensiktsmessig å legge vekt på risikovurderingsprosessen når man forstår begrepet risikovurdering og hvordan disse er implemntert i styringssystemer fra ISO standardene

2.4.4 Krav til IKT-tjeneste

Ledelsessystem for kvalitet – Krav gir tydelige krav til drift (NS-EN ISO 9001:2015). Den gir føringer for arbeidet i form av planlegging, implementering og å styre prosesser for å oppfylle kravene til levering av produkter og tjenester og til å implementere tiltakene som er bestemt for planlegging for å redusere risiko. Den tar spesifikt for seg styring av prosesser, produkter og tjenester levert fra eksterne (ISO 9001:2015). Gjennom å ha etablert et styringssystem for informasjonssikkerhet vil det fremgå hvilke krav som stilles til IKT-tjenesten (NS- ISO/IEC 27001:2013) (NS- ISO/IEC 27002:2013). I oppgaven vil kravene til IKT-tjenesten vurderes etter kriteriene fra disse standardene sees i sammenheng og vurderes i tråd med disse anbefalingene.

Leverandøstyring er en viktig dimensjon når man setter krav til IKT-tjenesten.
NS-ISO 9004:2018 følger opp med følgende føringer for leverandører og partnere og legger til grunn følgende
"Leverandører og partnere (hele avsnitt 6.4 er en slag veiledning til dette)
Det mest konkrete vil være at avtaler inneholder detaljer om samarbeidsforholdet og utveksling av informasjon (B.9 Kvalitetsstyringsprinsipp 8: Gjensidig fordelaktig samarbeid med leverandør)" (NS-EN ISO 9004:2018). Det er derfor hensiktsmessig å legge vekt på denne beskrivelsen når man forstår begrepet leverandørstyring.

2.4.5 Beslutningstaking

Aven påpeker viktigheten av beslutningstaking, spesielt i forhold til beslutningstakers gjennomgang og behov (Aven, 2015 s. 152), og at beslutningskriterier må være på plass (Aven T., 2015 s. 166). Videre påpekter han at risikoakseptkriterier må være definert (Aven T., 2015 s. 120). I oppgaven vektlegges derfor dette når man forstår begrepet beslutningstaking.

Som nevnt tidligere i teorikapittel vil risikoaksept i forhold til akseptabelt risikonivå være førende for hvordan man fatter beslutninger om tjenesteutsetting og hvilken kvalitet i beslutningsgrunnlaget som fremlegges til beslutning.

3 Metode

Metodekapittelet gir en presentasjon av de valg som er foretatt og gir oversikt over de valg som er benyttet for design og metode. For å besvare problemstillingen er metodevalg knyttet til problemstillingen. Den bygger på og besvarer hvilken risiko knyttet til risikofaktorer ved tjenesteutsetting og hvordan kvaliteten av disse vil påvirke risikostyringen gjennom temaoppbygging fra NSM sin Temarapport *"Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – en utdyping av området "beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet"*. Temarapportens anbefalinger (NSM, 2018a) gir veloverveide anbefalinger og grunnlag for hva som bør vurderes og drøftes i forbindelse med tjenesteutsetting. Temarapporten er benyttet som innspill til hvordan problemstillingen omhandles, hvordan den plasseres og og til slutt hvordan den beskrives gjennom inndeling av temaene som er lagt frem i Temarapporten (NSM, 2018a).

3.1 Studiedesign

Undersøkelsen tar utgangspunkt i kvaliteten på tjenesteutsetting, og hvilken risiko som er knyttet til temaene fra NSM Temarapporten (NSM, 2018a). For tema styring og kontroll i denne oppgaven er fokuset utvidet med styringsdimensjonen, og omhandler styring i tillegg til oversikt og kontroll over hele livsløpet fra NSM Temarapport (NSM, 2018a). Det er således en utvidet forståelse og bruk av styring og kontroll i denne oppgaven. I styring og kontroll kapitell sjekkes det om det gjennomføres forberedelser, planlegging, kontroll og styring av tjenesteutsettingen, om det er etablert ulike styringssystemer, og i hvilket omfang det gjennomføres risikostyring. Deretter vurderes det hvilken bestillerkompetanse som ligger til grunn for vurderingen av tjenesteutsetting. Fokuset videre er om det gjennomføres risikovurderinger, og av hvilken kvalitet disse har. Det vil videre vurderes hvilke krav som stilles til IKT-tjenesten, og om det vurderes risio og risikoens kvalitet knyttet til dette. Den neste risikofaktoren er av hvem, og med hvilket beslutningsgrunnlag, beslutninger tas ved tjenesteutsetting. Avslutningsvis vil det vurderes hvordan tjenesteutsetting foregår, hvordan det håndteres og i hvilken grad det påvirker kvalitet på risikofaktorene ved den helthetlige risikostyringen. Undersøkelsen vil gjennom prosessen ta for seg og koble problemstillingene opp mot teori, for å se hva som gjøres for å kunne få god kvalitet og kontroll på de empiriske dataene som er samlet inn, og på konklusjonen.

3.2 Intervjustrategi

For å få underbygge problemstillingen er det anvendt temaene anbefalt i Temarapport (NSM, 2018a). Disse temaene er relevante å få svar på, og for å vurdere kvaliteten ved en tjenesteutsetting av digitale IKT tjenester. Spørsmålene stilt under hvert tema søker å finne svar på kvaliteten på risikoen og risikostyringen ved tjenesteutsettingen, og om denne er helhetlig og bærekraftig.

Spørsmålene er stilt slik at informantene selv kan komme med sine betraktninger av tilstanden av kvalitet og risiko på de ulike spørsmålene. Spørsmålene er formulert slik at det gir grunnlag for utdyping. Der det er nødvendig med oppfølgingsspørsmål av underpunkter blir disse fulgt opp. Dette for å få belyst den helhetlige kvaliteten og risikoen ved tjenesteutsetting. Spørsmålene ble stilt generelt slik at informantene ikke ble ledet i sine svar.

3.3 Metodevalg

Hovedmetoden er kvalitativ metode med intervju (Blaikie, N. 2010).
Intervjuene er gjennomført med bakgrunn i at informantene jobber i offentlig sektor, enten stat eller kommune. De representerer sine respektive arbeidsplasser i offentlig sektor. De er intervjuet for å identifisere og kartlegge hvordan offentlig sektor ivaretar risiko og kvalitet både før, under og etter tjenesteutsetting. Disse representerer både statlig etater og statseide statsforetak, kommuner, kommuners interesseorganisasjoner og interkommunale foretak. Enkelte av disse er valgt med bakgrunn i at de har avsluttede kontrakter innen tjenesteutsetting, eller at de har tatt tjenester tilbake til Norge. Informantene er valgt ut fra relevans til tema. Intervjuene har foregått i et begrenset tidsrom i perioden juni til agust -19. Det er valgt 10 Informanter fra offentlig sektor, både statlig og kommunal, som er intervjuet, er virksomhetsledere, IT ledelse og sikkerhetsledere. Disse informantene er intervjuet med bakgrunn i deres kunnskap om tjenesteutsetting i deres etat, sektor eller selskap. Videre hadde det betydning hvordan tjenesteutsettingen var gjennomført og deres erfaring av i hvilken grad det har blitt håndtert, og om tjenesteutsettingen har vært vellykket.

3.4 Metodisk tilnærming

3.4.1 Datakilder

Det er brukt informasjon fra et utvalg av dokumenter og informanter. Oversikt over disse finnes i referanselisten i oppgaven.

Metode er valgt ut fra anvendt teori om standarder og bruk av disse (Engen O.A., m/fl, 2016) hvor Temarapport (NSM, 2018a) med sikkerhetsfaglige anbefalinger for tjenesteutsetting i denne sammenheng er benyttet som standard. Det er anvendt konkrete anbefalinger på tema fra Temarapport. Spørsmålene rapporten stiller blir brukt for å vurdere om risiko, og hvilke risikofaktorer ved en tjenesteutsetting, som vil gi et godt svar på om en tjenesteutsetting av digitale IKT tjenester vil ivareta nødvendig kvalitet i tjenesteutsettingen i offentlig sektor. Tema på spørsmål er: Styring og kontroll - Hvilken oversikt og kontroll på tjenesteutsettingen av tjenesten er gjort i forkant av tjenesteutsetting? Bestillerkompetanse - Hvilken bestillerkompetanse har etaten? Risikostyring - Er det gjennomført risikovurderinger? Krav til IKT-tjenesten - Hvilke krav ble stilt til IKT-tjenesten og leverandør? Beslutning om tjenesteutsetting - På hvilket nivå blir beslutningen om tjenesteutsetting fattet? (NSM, 2018a) Disse temaene utgjør hovedessensen av spørsmålene i intervjuguiden. Dette samsvarer godt med hensyn til anbefalingene fra ISO standarder (NS-EN ISO 9001:2015), (NS-EN ISO 31000:2009) og (NS-EN ISO 9004:2000).

Valg av informanter

Informantene er valgt ut med bakgrunn i sin kjennskap til tjenesteutsetting i sine respektive virksomheter. De kjenner til hvordan tjenesteutsetting foregår i deres etat eller sektor og har kunnskap om hvordan tjenesteutsettingen fungerer i etterkant av tjenesteutsettingen. Informantene har ulike organisasjons- og nivå-tilhørighet i sine virksomheter, men virksomheten er ulikt bygd opp og med ulik ansvarsfordeling som gjør at ulike roller ivaretar tilnærmet samme fokus rundt tjenesteutsetting. Ut fra deres rolle i virksomheten skal de ha kjennskap til viktigheten av helhetlig tankegang ved tjenesteutsetting. De er kjent med de elementer som bør inngå i tjenesteutsettingen, som virksomhetsstyring, nødvendige forberedelser, planlegging, risikovurderinger, bestillerkompetanse, krav til tjenesten og beslutningstakere.

Sektor	**Virksomhet**	**Stilling og Relevant erfaring**	**Omtales i oppgaven som**	**Type intervju**
Kommunal sektor	Kommune	Direktør digitalisering og IT: 40 års erfaring innen IKT, på alle sider av bordet på IT, 10 år med tjenesteutsetting	Informant 01	Individuell

Kommunal sektor	Kommunalt selskap	Kvalitets- og sikkerhetsansvarlig: Erfaring med IT og datakommunikasjon og datasikkerhet/informasjonssikkerhet over 20 år. Har vært rådgiver og deltatt i risiko- og sårbarhetsvurdering, samt foredragsvirksomhet innenfor tema.	Informant 02	Individuell
Kommunal sektor	Kommunalt selskap	Daglig leder: IT digitalisering og tjenesteutsetting i over 20 år, og IT drift Sikkerhetsansvarlig: Sikkerhet de siste 15 år	Informant 03	Dobbel
Kommunal sektor	Kommunal organisasjon	Områdedirektør forskning, innovasjon og digitalisering: Topplederfunksjoner siden år 2000 Avdelingsdirektør: IT sjef og utviklingsansvarlig og erfaring fra drifts og utvikling, konsulent i større organisasjoner offentlig og privat	Informant 04	Dobbel
Kommunal sektor	Kommune	Teknologidirektør: Jobbet med IT siden 1998, kvalitetsstyring og sikkerhet i 20 år	Informant 05	Individuell
Statlig sektor	Statlig foretak	Viseadministrerende direktør: Mer enn 20 års erfaring innen sektoren Juridisk direktør: Mer enn 15 års erfaring innen sektoren.	Informant 06	Dobbel
Statlig sektor	Statlig selskap	Leder Sikkerhet og Juridisk: Erfaring på sikkerhetsområdet i offentlig sektor nær 20 år, de siste 13 år som sikkerhetssjef.	Informant 07	Individuell
Statlig sektor	Statlig etat	Fagdirektør: Mer enn 30 år på IT og kommunikasjonsteknologi. Lang erfaring fra store organisasjoner. Ansvar for å implementere mange store systemer på alle nivå.	Informant 08	Individuell
Statlig sektor	Statlig etat	Seksjonsleder innovasjonsseksjonene i virksomhetsavdelingen: Nær 30 års erfaring innen IT på varierte fagområder, i tillegg ledet arkitektur- og sikkerhet i flere perioder. Erfaring både fra offentlige virksomheter og på kundesiden som leverandør.	Informant 09	Individuell
Statlig sektor	Statlig selskap	Service Manager: Erfaring fra IT i ulike roller i offentlig sektor i over 35 år. Flere år som avdelingsleder.	Informant 10	Individuell

Tabell 2: Oversikt over informanter

3.5 Intervjuguide

Intervjuguiden ble satt i henhold til tidligere nevnte tema fra Temarapport (NSM, 2018a). Intervjuguiden er vedlegg til denne oppgaven. Spørsmålene er satt inn under de tema de passet best, men flere av spørsmålene som er besvart under tilsvarende punkt i empiri vil bli drøftet under flere andre tema og spørsmålsstillinger i drøftingskapitlet.

3.6 Gjennomføring av intervju

Ved intervjuet er det valgt å følge en intervjuguide som består av noen hovedtema med underspørsmål. Intervjuene ble gjennomført i samtaleform hvor spørsmålene ble stilt og besvart. I noen tilfeller var det relevant å stille tilleggsspørsmål for å få frem eller få konkretisert informantenes svar. Alle informantene ble stilt de samme hovedspørsmålene. Det ble ikke stilt ledende spørsmål. Der det var nødvendig å stille tilleggsspørsmål ble disse stilt i henhold til casestudie, valgte temaer for spørsmålene, og hva som ønskes besvart under hvert tema og spørsmål.

I forkant av intervjuene ble det sendt ut en henvendelse om å stille som informant med informasjon om forskningsoppgaven og hvilket tema som skulle belyses. Intervjuene ble gjennomført hos den enkelte virksomhet. Sted ble valgt ut fra at de skulle føle trygghet og ikke få ekstra belastning med å måtte forflytte seg til annet sted. Varigheten på intervju var estimert til 1,5 time, men varierte fra 1-2 timer.

I flere av intervjuene stilte det to informanter fra virksomheten, et såkalt dobbeltintervju. Både intervjuene med en og to informanter fungerte greit. Der det var to utfylte disse hverandre på en god måte.

3.7 Datamateriellets kvalitet

Det finnes allerede tilgjengelig informasjon på tilstanden til enkelte tjenesteutsettinger. Dette er positivt og førte til at det syntes nødvendig å forske videre på temaet.

En negativ side ved å ha forkunnskaper rundt et tema man ønsker å forske videre på, er at kjennskapen til og kunnskapen om eksisterende hendelser kan gjøre forskeren forutinntatt med tanke på vinklingen av tema i oppgaven. Dette er forsøkt hensyntatt ved å plukke informanter fra et bredere sett av virksomheter innenfor offentlig sektor, både kommunal og statlig sektor.

3.7.1 Validitet

Intervjuene har foregått i et begrenset tidsrom, og hos et begrenset antall roller av medarbeidere. Det er i all hovedsak intervjuet ulike direktører/ledere/daglige ledere, enkelte IT ledere og i noen tilfeller sikkerhetsledere. Det kan således være en iboende trussel at dataanalysen bygger på et for lite utvalg av ulike roller og nivå i virksomheten, og at resultatet derfor kan være bedre eller verre i forhold til dagens nåsituasjon for tjenesteutsetting. Det var ikke alltid like enkelt å få de svar som var forventet informasjon. Om det skyldes manglende informasjon eller kunnskap hos informantene er ikke kjent, eller ikke ønsket å uttale seg.

3.7.2 Reliabilitet

Svarene fra informantene ble notert ned underveis i intervjuet og svarene fra hver informant er lagt i et eget dokument. Det ble ikke benyttet opptak. Svarene ble stort sett gjengitt fra intervjuer for å sikre at informantene var oppfattet riktig. Noen ga lange svar og ønsket å få frem mange sider av problemstillingen, andre var korte og konsise i sine svar.

Påliteligheten til de svarene som fremkommer, og om andre til komme til samme resultat, beror på om man benytter de samme informantene, om samme tema belyses og om tilsvarende spørsmål blir stilt.

3.8 Etiske betraktninger

Miljøet for blant annet offentlig sektors digitale IT ressurser og sikkerhetsledelse i Norge er relativt lite. Kandidaten har således jobbet med og har relasjoner til enkelte av informantene i kraft av kollegaer i tidligere arbeidsforhold. Kandidaten har således kjennskap til enkelte av informantene fra før.

Kandidaten har tidligere jobbet i en av virksomhetene informanten representerer, men dette var før større satsning på digital tjenesteutsetting. Kandidaten har imidlertid vært medlem i interrimstyre i kraft av sin rolle, noe som senere ble til et hovedprosjektet hvor blant annet digital IKT tjenesteutsetting ble gjennomført.

Kandidaten har imidlertid ikke jobbet dedikert med eller sammen med noen av informantene i sammenheng med digital IKT tjenesteutsetting.

4 Empiri

Problemstillingen belyser risikoen knyttet til kvalitet ved tjenesteutsetting. Første spørsmål i problemstillingen belyser på hvilken måte offentlig sektor vurderer risiko knyttet til tjenesteutsetting av digitale IKT-tjenester. Det neste spørsmålet er hvordan risikovurderingene innvirker på kvaliteten av tjenesteutsettingen av digitale IKT-tjenester. De tre underliggende forskningsspørsmålene har fokus på risikofaktorer, på hvordan de er knyttet til risikovurderingene, og hvilke av faktorene som veier tyngst i beslutningsprosessene. Hovedspørsmålene vil vektlegges under drøftingsdelen. De underliggende spørsmålene vil bli vektlagt under de enkelte spørsmålene hvor de hører hjemme i empiridel og deretter drøftet i drøftingsdel.

Funnene er hentet inn gjennom intervjuer, og empirien er organisert etter samme struktur som intervjuguidens spørsmål som ble stilt til informantene. Intervjuguidens spørsmål er valgt med bakgrunn i at det vil fungere i forhold til problemstillingen, men med hensyn til kvalitet og risiko knyttet til tjenesteutsetting.

Hovedtemaene med underliggende spørsmål er delt opp etter modell fra NSM Temarapport (NSM, 2018a). Hovedtemaene er delt i Styring og kontroll, Bestillerkompetanse, Risikovurderinger, Krav til IKT-tjenesten og Beslutningtaking. Deretter samles svarene fra hver informant under hvert spørsmål som ble stilt i intervjuet. Funnene blir presentert oppsummert fra alle informantene. Enkelte utsagn fra informanter vil presenteres i sin helhet med henvisning til informantnummer.

4.1 Hvordan behandles styring og kontroll ved tjenesteutsetting?

Når det gjelder styring vil oversikt og kontroll over hele livsløpet drøftes i dette kapittelet. For å oppnå styring er det nødvendig å skaffe oversikt over og få kontroll på hele livsløpet til tjenesteutsettingen. I NSM sin temaveileder under punktet: oversikt og kontroll på hele livsløpet (NSM, 2018a), vektlegges det at det er belyst hvilke forutsetninger som er tatt og hvilke vurderinger som er gjort i forkant av tjenesteutsettingen. Det vil derfor belyses om og med hvilken kvalitet virksomhetene har på risiko og styringen av livsløpet til tjenesteutsetting. Kapittelet er strukturert etter de spørsmål som er stilt informantene.

Hva er hovedformålet med den digitale IKT tjenesteutsettingen?

Hovedformålet med tjenesteutsetting er at det kan gi økonomiske fordeler for en virksomhet. Det har vært spekulert i om enkelte virksomheter kan ha sett for ensidig på økonomien. I innledningen til NSM Temarapport fokuseres viktigheten av at tjenesteutsetting kan gi bedre sikkerhet og mer stabile og tilgjengelige tjenester for den enkelte virksomheten. (NSM, 2018a). Videre påpekes det i Temarapporten at *"Tilsvarende eller høyere nivå på både tjenestekvalitet og IKT-sikkerhet bør være en målsetting ved tjenesteutsetting."* (NSM, 2018a s 9). Funnene viser at det er stor variasjon på hva som er hovedformålet med tjenesteutsettingen. Hovedformål har for flere av virksomhetene vært at de skal dekke områder hvor tjenester kun kan leveres som skytjenester og det å få prøve markedet. For andre har målbildet vært mer uklart. Konkurransekraft, innovasjon og effektivisering oppgis av en informant som hovedårsaker til konkurranseutsetting, og ikke hovedsakelig økonomi. I tillegg oppgir de tilgang til ny teknologi og evne til modernisering som en viktig målsetting. En annen informant opplyser at hovedformålet er basert på, og valgt ut med bakgrunn i kompetanse, skalerbarhet, fleksibilitet og profesjonalitet. Flere har pris/økonomi og kvalitet som selve formålet. Flere av informantene uttaler at kvalitet vil veie tyngst, andre presiserer at det er økonomi og den raskeste vegen til målet som er førende. Innenfor statlig sektor er markedet, ansvarliggjøring av leverandørene, og behovet for fornyelse av avtaler vært førende for flere informanter. Innenfor kommunal sektor er variasjonen for formålet større enn hos statlig sektor.

Hvilke forberedelser i forkant av tjenesteutsetting?

Når det gjelder forberedelser anbefaler NSM Temarapport at *"det utarbeides detaljerte forutsetninger for tjenesteutsettingen, samt at det gjøres nødvendige vurderinger av om tjenesten kan gjennomføres og eventuelt hvordan"* (NSM, 2018a s 11). For å oppnå det vil kvaliteten på forberedelsene være avgjørende i forhold til å avdekke risikoprofil i hele verdikjeden. Det er nødvendig å få frem de viktigste og mest kritiske momentene basert på risiko, kort sagt: hva er viktig å sikre.

Det er stor variasjon i hvordan informantene svarer på hvilke forberedelser som gjøres. Flere informanter fra kommunal sektor oppgir at det hovedsakelig er obligatoriske risikovurderinger de gjennomfører som forberedelser. Enkelte oppgir at det i tillegg gjennomføres konsekvensvurderinger knyttet til personvern, såkalt personvernkonsekvensvurderinger. Flere informanter vektlegger at det tidligere i liten grad

ble gjort forberedelser, og at i den grad det gjøres forberedelser er de ikke er knyttet til styring av tjenesteutsettingen. Forberedelsene har ofte blitt gjort på et dårlig grunnlag, noe som igjen medførte et altfor dårlig beslutningsgrunnlag. Det viser seg også mangler knyttet til at det ikke er løftet opp på ledernivå i tilstrekkelig grad. Flere av virksomhetene som har hatt uheldige tjenesteutsettinger oppgir at erfaringen har medført at det er innført nye føringer for hvordan forberedelsene skal foregå. Flere påpeker imidlertid at det fortsatt er forbedringspotensiale.

En informant oppga at de ikke hadde kompetanse på området tjenesteutsetting i det hele tatt. I tillegg uttaler informanten at det heller ikke er noen overbevisende dokumentasjon på hvorfor man skulle tjenesteutsette, det er både lite konkret og ikke forankret i ledelsen. Denne informanten opplyser videre at det i pågående tjenesteutsetting er laget en strategi, men at de benytter et eksternt selskap til dette. Flere opplyser at det mangler prosesser for forberedelser, men at det utarbeides en kravspesifikasjon og en risikovurdering. Noen ser på behov og innhenter råd. Det kommer frem at det har foreligget urealistiske tidsplaner. Tempoet og at det gikk for raskt til slik at styring og kontroll manglet oppis som annen grunn til manglende forberedelser. Hos disse er det nå etablert et eget oppfølgingsregime av tjenesteutsetting for de pågående tjenesteutsettingene. For en informant ivaretas forberedelser ved at det skjer både på strategisk, taktisk og operasjonelt nivå. En annen informant opplyser at dette gjennomføres gjennom en prosjektmodell, med en konseptfase, en gjennomføringsfase og en prosjektfase. En tredje informant oppgir at de samler inn og systematiserer, og på denne måten forbereder tjenesteutsettingen. Funnene viser at det kun er én virksomhet som har fått laget en strategi på hva tjenesteutsettingen skal omfatte.

Funnene viser at tre av ti informanter gjør forberedelser.. Det viser en mangel på praksis. God risikostyring oppnås ved å *"koordinere aktiviteter for å rettlede og kontrollere en organisasjon med hensyn til risiko (2.1)"* [SN-ISO Guide 73:2009, definisjon 2.1]. Det innebærer gode forberedelser med etablering av strategi eller formaliserte prosesser i arbeidet med forberedelser til tjenesteutsetting Her er det en avstand mellom teori og praksis.

Hvilke prosesser gjennomføres, før, under og etter tjenesteutsetting?

Funnene fra prosesser er organisert felles for kommunal og statlig sektor. Prosessene før og under er samlet, mens prosessene i etterkant er skilt ut i eget avsnitt. Noen av informantenes opplysninger om sin virksomhet er skilt ut i sin helhet og gjengitt med henvisning til informantnummer.

Det fremkommer av funnene at det er flere ulike måter å styre prosessene for avklaring om tjenesteutsetting på. En viser til at de har engasjert et selskap som de skal samarbeide med, og som det er tenkt skal lede de gjennom alle prosessene ved tjenesteutsetting, både å kvalitetssikre prosesser og kontrakter, og å gi juridisk bistand. Disse har ikke etablert noen prosesser, men har startet arbeidet med å utarbeide prosesser.
Flere påpeker at de skal utarbeide styrende dokumenter hvor prosessene skal implementeres. Hos en virksomhet er praksis bra, men man har ikke formalisert og dokumentert prosessene godt nok. Hos flere virksomheter baseres prosessen på behovskartlegging, og at tjenesteutsettingen gjennomføres i henhold til ordinær anskaffelsesprosess, risikovurdering knyttet til informasjonssikkerhet, personvern og kost/nytte av hvilken løsning som er best. En annen virksomhet gjennomfører prosesser med verdivurderinger og tilhørende risikovurderinger ut fra hvilken informasjon som behandles og hvilken løsning det skal støtte opp under. Det gjøres imidlertid i noe varierende grad i praksis, men er i sterk bedring. En annen informant viser til at prosessene ikke alltid er like godt gjennomtenkt når behovene kommer til IT. Det gjennomføres derfor kvalitetssjekk og vurderinger for å sikre arkitektur, sikkerhet, integrasjon og driftsrammeverk av IT. De ser imidlertid at kjøp kan foregå av fagmiljøene i forkant på et litt svakt beslutningsgrunnlag. Dette viser at det er svært få innenfor kommunal sektor som har etablerte prosesser som er forankret i styringssystemer til tross for at flere mener de allikevel har en god praksis.

Det er stor variasjon i hva informantene oppgir av prosesser som brukes. Flere r at det jobbes med å etablere en helhetlig prosess for det strategiske i virksomhetene. Enkelte av virksomhetene har ressurser som håndterer hver enkelt prosessområde, og har anskaffet verktøy for prosessarbeidet, men ikke implementert dette. Andre forteller at virksomheten definerer hvilke tjenester de vil ha, og stiller krav til disse, samt at det blir etablert en liten kjernegruppe som har samlet kravene. Andre igjen opplyser at man kun av og til gjennomfører kvalitetssjekker under arbeidet med tjenesteutsetting, eller at det stilles krav til tjeneste, leverandør og sikkerhet, både taktisk og operasjonelt, eller at virksomhetene tidligere ikke har hatt prosesser for tjenesteutsetting, men at de nå har etablert prosesser for tjenesteutsetting. Sistnevnte uttaler at *"Det er etablerte prosesser for styring og kontroll av tjenesteutsetting. Konsernrevisjon følger nå alle program hvor elementer kan tjenesteutsettes. Det er et eget regime for nye programmer som skal tjenesteutsettes fordi disse er store. En intern tjenesteleverandør skal lage en strategi for bruk av markedet og tjenesteutsetting. Blant annet om det er hensiktsmessig å bruke markedet og hvordan dette skal gjøres."* [Informant

06]. En annen informant uttaler *følgende "Prosjektet kjøres real life. Det er stort og omfattende og vi har ikke tid til å innhente alle typer kunnskapsinnhenting og opplysninger i forkant. Beslutninger ble tatt der og da med det kunnskapsnivået vi hadde på det tidspunktet. Vi måtte støtte oss på eksterne selskaper og også på arbeidskraft fra hele verden. Utviklingen skjedde i København og i store miljøer over heleverden. Mange av disse kjenner ikke til norsk lovverk som for eksempel sikkerhetsloven. Staten hadde ikke kompetanse på tjenesteutsettingsområdet selv, og var avhengig av å ha tillit hos innleide med spesialkunnskap."* [Informant 08]. Dette er et type funn som kun er observert fra denne ene informanten.

For prosesser i etterkant av tjenesteutsetting viser funnene variasjoner på om det er etablert prosesser for oppfølging av leverandørene. En informant oppgir at virksomheten har etablert faste arenaer for oppfølging av de største leverandørene. Prosesser på hendelses-, problem- og avvikshåndtering er etablert. Flere av informantene opplyser at de følger tettere opp disse prosessene mot de store leverandørene som ivaretar kritiske systemer for dem. En knytter det til ledelsens gjennomgang, og at det gir noen føringer for hvordan det skal ivaretas. En annen informant forteller at det i etterkant følges opp i liten grad, og at de ikke har systematisk tilnærming til oppfølging i de ulike systemene. Informanten mener de er umodne både på leverandørstyring og på å stille krav til leveranser. En sier det er laget et system for å følge opp anskaffelser med tjenesteutsetting, men at de mangler den helhetlige biten. Etter en uheldig tjenesteutsetting har det blitt en høyere bevissthet på at ansvaret ligger i toppledelsen. Dette har derfor fått økt fokus. Informanten forteller at *"Eier har også bevisst satt ressurser med kompetanse på IKT inn i styret. Det er et helt annen fokus som følge av kompetanse i styret og i ledelsen som nå ser dette. Det er bevissthet på hvilke spørsmål som må stilles."*. [Informant 06]. Funnet viser en økt modenhet og samsvarer godt med modenhetsmodellen for outsourcing og det at man *"2) utvikler og integrerer ressurser og kompetanse som understøtter den strategiske kjernen"* (Sæther, Hans Solli 2016)

Informanten hos et statlig selskap oppgir at leverandørene følges opp gjennom målinger, faste møter og kvalitet på innhold i leveransene. I alle faser har anskaffelsesavdelingene egne ressurser for hver kategori av leveranser. En seksjonsleder hos en statlig etat beskriver at det er varierende oppfølging og evaluering av tjenesteutsetting. Service manager hos et statlig selskap forteller at de *"implementerer kontrakter og kjører transisjonsprosjekter hvor kontrakten implementeres på alle stedene den berører. Vi kjører deretter opplæring på de nye*

ressursene på hva en ny kontrakt inneholder" [Informant 10]. Denne virksomheten har således god kontroll på sine utkontrakterte tjenester.

En av kommunene redegjør for en form for partnerskap som styringsmodell hvor det er etablert en deling mellom rådgivningsenhet i kommunenes administrasjon og de enkelte fagsektorene. Videre forteller informanten at *"Denne øvelsen er imidlertid krevende og trenger modning hos sektoransvarlig. Det er videre etablert prosesser med foranalyse hvor gevinstrealiering vurderes, konseptfase som er en arena med tverrfaglig kompetanse som ser på gevinstrealisering plan og samordning, og en planleggingsfase hvor man må ha alle sjekkpunkter grønne for å gå videre. Deretter vurderer tverrfaglig kompetanse sammen grønt lys for hvilken type utvikling og anskaffelse man ønsker å gjennomføre. Til slutt er det en avslutningsfase med realisering av tjenesteutsettingsformen som er valgt."* [Informant 01]. Deretter gjøres en onboarding for alt innleid personell og det jobbes tett med leverandøren om videreutvikling. Denne prosessen oppleves vanskelig når det er store leverandører med ulik håndtering av de innspillene som gis gjennom prosessen og informanten mener det kunne vært utført en bedre leverandøroppfølging i disse prosessene. Direktøren viser til *"anskaffelsesmetoder som er uhensiktsmessige og mener det å drive innovasjonspartnerskap er et område man ønsker seg mer av ved å gå i dialog med leverandører som er gode på digital utvikling. Leverandørstyring før under og etter leveransene er en viktig dimensjon og vektlegges i kommunen"* [Informant 01]. Informantens virksomhet har en veldokumentert styring når det kommer til valg av tjenester og tjenestemodell. Til tross for dette opplyser direktøren om at det fortsatt er behov for å jobbe mer med modellen, spesielt opp mot leverandørene og med anskaffelse, for å få det godt innarbeidet og øke modenheten.

Det er ikke funnet store forskjeller mellom statlig og kommunal sektor når det gjelder prosesser før, under og etter tjenesteutsetting. I begge sektorene er det i de aller fleste tilfeller mangel på modenhet ved tjenesteutsetting. Hos begge sektorene er det variasjoner, men bevisstheten på styring og kontroll ved tjenesteutsetting viser at det er et forbedringspotensiale. Virksomheter som har tjenesteutsatt over tid viser en større modenhet enn der de har lite erfaring med tjenesteutsetting. Det fremkommer at de som har hatt uheldige tjenesteutsettinger som er trukket tilbake, har eller har under etablering, styringssystemer og prosesser for å ivareta tjenesteutsettingen og skaffe seg oversikt over hele livsløpet.

Virksomhetene ser behovet for planlegging av tjenesteutsetting. Likevel fremkommer det at det planlegges fra gang til gang og at det ikke er etablert klare føringer hos de fleste virksomhetene. Der de har hatt uheldige tjenesteutsettinger har de etablerte prosesser for fremtiden, men de forteller at det fortsatt er umodenhet og krever tydeligere implementering. En kommune er kommet langt i arbeidet med styring og kontroll, men forteller at det er et forbedringspotensiale. Flere statlige selskaper som har holdt på med tjenesteutsetting over tid viser en større modenhet og har flere etablerte prosesser for styring og kontroll. Funnene viser at det er et stort forbedringspotensiale for å etablere styringsprosser slik at det oppnås kontroll ved tjenesteutsetting. Dette gjelder både i forkant av, for oppfølging i avtaleperioden og i etterkant for avslutning av tjenesteutsetting. Deretter må det implementeres i virksomhetens styringssystemer.

Hvilket kunnskapsnivå har ofentlig sektor og foretas kunnskapsinnhenting?

Ved flere anledninger er tjenesteavtaler trukket tilbake og tjenesten hentet tilbake til virksomheten. Flere hendelser viser at der det har vært for dårlig kunnskap i virksomheten vedrørende hva og hvordan en tjenesteutsetting bør foregå, og som har ført til uheldige tjenesteutsettinger. Funnene viser variasjon på kunnskapsnivået om tjenesteutsetting i offentlig sektor.

I en av virksomhetene opplever flere at den samlende kunnskapen er god. Der man mangler, eller har mangelfull kunnskap, kjøpes det inn spisskompetanse på områder hvor det er behov for det. Funnene viser at man da er godt fornøyd med totalinnhentingen av kompetanse. Flere av funnene viser at virksomhetene opplever at de i varierende grad har nødvendig kunnskapsnivå og modenhet på tjenestutsetting. Flere av informantene oppgir at de må ut i markedet for innhenting av kunnskapen. Kunnskapen innhentes fra leverandører og relevante konferanser. Hos en av virksomhetene er kunnskapsinnhenting meget desentralisert og det finnes svært lite formalisert kvalitetssjekk ute i organisasjonene. Kunnskapsnivået oppfattes på denne måten fra en annen informant, og denne vektlegger at det *"Handler i stor grad om manglende ressurser. Modenheten er lav, viljen er stor og evnen er lavere. Handler om kompetanse, men mest av alt om kapasitet"* [Informant 05]. En Kvalitets- og sikkerhetsansvarlig uttaler at *"Kan se ut som man lytter til de positive sidene som engasjerte innleide legger frem, mindre lytting til de mulige negative sidene som således ikke kommer frem."* [Informant 02]. Slik sett legger flere av virksomhetene opp til at leverandørene i stor

grad kan styre tjenesteutsettingen og tar ikke ansvaret for at de har riktig kunnskap for å utarbeide gode beslutningsgrunnlag for ledelsen. Sett i lys av at en informant oppgir at hans *"opplevelse er at leverandører gjennomgående ikke har like god kompetanse"* [Informant 01] kan det være risiko knyttet til det å basere seg ensidig på den kunnskapen leverandørene besitter om tjenesteutsetting.

Fra et statlig foretak oppgis det at *"Kunnskapen var i linjen, men det er nå økt kunnskapsnivå og bevissthet i ledelse og styre. Avklaring og beslutninger blir i større grad trukket opp i styret."* [Informant 06]. Gitt deres uheldige tjenesteutsetting kan det tyde på at kunnskapen heller ikke var god nok i linjen da det ikke ble utført de nødvendige aktiviteter for å ha kontroll over hele livsløpet. Videre forteller informanten at *"Linjen informerte heller ikke alle forhold oppover i organisasjonen eller ga et godt nok beslutningsgrunnlag. Det medførte at ledelse og styre ikke var i stand til å fatte de riktige beslutningene."* [Informant 06]. Dette endte med at tjenesteavtalen ble avsluttet under implementeringsløpet.

En leder for Sikkerhet og Juridisk opplyser at *" Kunnskapsinnhenting foregår på to nivåer. Det ene skjer i regi av innkjøpsavdelingen. Å forstå modenhet i markedet om leveranser, produkter, leveranderører, samt hvor man finner disse leverandørene. Det andre går direkte mot det å komme inn i prosessen, undersøke leverandørene, due diligens, bakgrunnsundersøkelse."* [Informant 07]. En annen informant opplyser at *" Vi har bygget opp tydeligere sikkerhetsmiljøer som ivaretar kunnskapsnivå og -innhenting, samt etablert en egen sikkerhetsseksjon. Disse trekkes inn i kravspesifikasjonen. Det avgjørende er å forstå bruken av tjenesten. Risikovurdering er en kontinuerlig prosess."* [Informant 09]. Begge disse to vitner om en virksomhet som har et bevisst forhold til tjenesteutsetting og hva som kreves av kunnskap for å forstå bildet rundt det.

Fagdirektøren i et statlig etat oppgir at *"prosjektet kjøres real life. Det er stort og omfattende og vi har ikke tid til å innhente alle typer kunnskapsinnhenting og opplysninger i forkant. Beslutninger ble tatt der og da med det kunnskapsnivået vi hadde på det tidspunktet."* [Informant 08]. Det kan tyde på liten modenhet i etaten knyttet til tjenesteutsetting.

I hvilket omfang blir det kartlagt usikkerhet?

Usikkerheten knyttet til tjenesteutsetting er en vesentlig faktor. Det kan knyttes risiko til enhver anskaffelse. Usikkerhetsfaktorer som er knyttet til tjenesteutsettingen er viktige

risikofaktor. Det kan få store konsekvenser for kvaliteten dersom de ikke blir hensyntatt. I forbindelse med anskaffelser vil det være risiko for usikkerhet. Dersom det ikke blir identifisert hvilken usikkerhet som kan oppstå, vil det kunne gi en større sannsynlighet for at risikofaktorer ikke blir plukket opp og håndtert.

Avsnittet viser de funn som fremkom fra informantene på om usikkerhet blir håndtert ved tjenesteutsetting.

De fleste informantene oppgir at usikkerhet ikke blir kartlagt eller håndtert skikkelig. I beste fall skjer dette av og til, men det gjøres i utgangspunktet så langt som det er mulig i forkant av en tjenesteutsetting. Flere av informantene er ikke kjent med om det innhentes informasjon om usikkerhet. En informant gir uttrykk for at det i enkelte tilfeller innhentes grundig informasjon om usikkerhet. En annen informant opplyser om at det blir vurdert usikkerhet gjennom risikoanalyser. Det har videre blitt fortalt av en områdedirektør at de vurderer leverandørene og deres løsning i alle ledd i løpet av anskaffelsesprosessen. Vedkommende forteller at *"Jeg er opptatt av at usikkerhet må identifiseres og regner med at det blir gjennomført."* [Informant 04]. En annen informant oppgir at *"Usikkerhet blir kartlagt så langt man klarer i forkant. I etterkant vil man kunne se området som burde vært vurdert."* [Informant 06]. Leder for Sikkerhet og Juridisk i et statlig selskap presiserer at *"Usikkerhetsvurdering består av to ting, risiko (nedside) og muligheter (oppside). Vi er flinke til å se på risiko, men ikke så gode på å se på mulighetsvurderingene."* [Informant 07]. En annen informant forteller *"Det ble ikke avklart noen usikkerhet, det ble aldri bevisst tjenesteutsatt og det ble brukt utenlandsk arbeidskraft til å gjøre jobben."* [Informant 08]. Et av de viktigste funnene er at det understrekes fra de fleste at usikkerhet ikke er vurdert i anskaffelsesprosessen.

Hvilke kvalitetskrav stilles?

Det er gjennomgående slik at kvalitetskrav enten ikke er etablert eller at de skal påbegynnes. Kun tre av ti har jobbet med eller har etablert noen form for kvalitetskrav. Den ene av de to informantene som har etablert kvalitetskrav forteller at *"Kravene til selskapet hvor det er hovedkrav er at hvis du skal levere en tjeneste skal man som minimum være sertifisert etter 27001 eller 9001. Kontrollkravene er delt inn i sju områder; informasjonssikkerhet, personvern, kvalitet, antikorrupsjon, hvitvasking, samfunnsansvar og forretningskritiske krav til tjenestene."* [Informant 07]. Den andre informanten uttaler følgende om kvalitetskrav

"Innen sikkerhet var det enkelte krav som gikk på geografi. Juridisk enhet er alltid involvert med tanke på juridiske spørsmål og avtaletekst. Det ble stilt krav til at leverandøren måtte være tilstede i Skandinavia og tilby nøkkelpersonell med skandinavisk språk. Vi brukte de 500 kravene som utgangspunkt i blant annet sikkerhetspolicyen som ligger til grunn for det man gjør innenfor området og innenfor tjenesteutsetting." [Informant 10]. Disse to virksomhetene er begge statlige selskaper som har erfaring med tjenesteutsetting over tid. Dette viser at det er modenhet i de to virksomhetene på å stille kvalitetskrav ved tjenesteutsetting. Den tredje informanten viser til *"Det er tre viktige kvalitetskrav; konfidensialitet, integritet og tilgjengelighet. I noen tilfeller stilles fagspesifikke krav og vi stiller generelt sikkerhetskrav til leverandører. Under utvikling og etablering er det et eget styringssystem for informasjonssikkerhet. Anskaffelsesorganisasjonen har eget kvalitetssystem."* [Informant 09]. Dette anses ikke å være tilstrekkelig til bruk som kvalitetskrav ved tjenesteutsetting.

I hvilken grad gjennomføres leverandørstyring?

Leverandørstyring følges stort sett opp av alle virksomhetene. Dette gjøres imidlertid i svært varierende grad. Flere uttaler at det er ulik oppfølging og fokus på hva som følges opp avhengig av om det er fagsektorer og IT avdelinger som følger opp.

For kommunal sektor er oppfølgingen for de fleste delt mellom IT avdelingen og fagsektoren. Dette kan utgjøre en risiko med tanke på den helhetlige oppfølgingen, og risikoer kan på bakgrunn av det bli oversett. En informant uttaler at det finnes et stort forbedringspotensiale for leverandørstyring. Kvalitets- og sikkerhetsansvarlig beskriver en tilnærming som avviker fra de øvrige informantene *"Nå er en del av strategien å sette ut leverandørstyringen til en integratorrådgiver. De skal lære opp organisasjonen i etterkant. Det er fire moduler i leveransemodellen. Disse er å etablere tjenesteintegrator, moderne IT tjenester (drift) og sikkerhetstjenester. Den fjerde: intern tjenesteforvaltning (tjenesteutvikling) er ikke en del av det. I integratorrollen ligger IT leverandørstyring, program- og porteføljestyring, service management, application management, kontinuerlig forbedring, skyrådgivning, transformasjonsstrategi og lisensrådgivning."* [Informant 02].

På statlig side fremkommer det at flere av intervjuede virksomheter enn på kommunal side har leverandørstyring. Årsaken til det kan ligge i at flere på statlig side har oppgitt at de har holdt på med tjenesteutsetting over lengre tid. På kommunal side fremkom det at det først i den senere tid har blitt mer tjenesteutsetting. Det er imidlertid interessant at en fagdirektør i

statlig etat fremhever at *"Det er ikke gjort noen bevisst tjenesteutsetting utover det at det ble inngått en nøkkelavtale med hovedleverandør hvor de hadde alt ansvar for videre underleverandører. Hva man finner i den kjeden har vært vanskelig å følge opp."* [Informant 08]. Det var forventet en større modenhet hos denne etaten da de har tjenesteutsatt et stort porteføljе gjennom flere år. Dette anses ikke som en systematisk oppfølging av leverandør fra kundens side.

4.2 I hvilken grad legger man til grunn bestillerkompetanse?

Bestillerkompetanse kan være avgjørende for om tjenesteutsettingen blir vellykket eller ikke. Tjenesteutsettingen er avhengig av god bestillerkompetanse i virksomheten for at den skal bli vellykket. NSM sier i sin Temarapport *"Svak bestillerkompetanse kan medføre at virksomheten anskaffer IKT-tjenester uten tilstrekkelig kartlegging av behov, og kan gi utfordringer med å stille gode krav til blant annet IKT-sikkerhet ovenfor leverandør."* (NSM, 2018a s. 13). For å oppnå god kvalitet på bestillerkompetanse er det viktig at alle kompetanseområdene innehar ressurser med IKT-kompetanse (NSM, 2018a).

Det er variasjon i hvilken bestillerkompetanse informantene oppgir at virksomhetene innehar. Flere informanter oppgir at bestillerkompetansen i deres virksomhet er god. Informantene henviser til og oppgir ulike grunner for hva de legger i god bestillerkompetanse. En oppgir at det er et godt IT-miljø, men presiserer at det godt kunne vært supplert med kompetanse fra flere fagmiljø for å kunne blir mer profesjonelle når det kommer til tjenesteutsetting. En annen begrunner at bestillerkompetansen er god med at de har en egen strategisk ressursperson med god forståelse for virksomhetsarkitektur, og henviser til at de har ganske god faglig og teknisk bestillerkompetanse. Enkelte informanter sier bestillerkompetansen er varierende i virksomheten, men at det stadig bedres. Det uttrykkes fra andre at bestillerkompetansen skal forbedres, at de mangler den i dag, eller at det er meningen at den skal utvikles. Videre nevner flere at de jobber mye med å beskrive behov, og de ser økende grad av bedring. En informant sier at *"de har liten eller ingen egenkompetanse på bestillerkompetanse i Staten"* [Informant 08]. Det er viktig at den enkelte virksomhet selv tar ansvaret for å ivareta bestillerkompetansen.

En direktør forteller at *"Vi innehar en tverrfaglig bestillerkompetanse definert gjennom styringsmodellen. Denne tillater ikke manglende kompetanse på IT. Teamene settes sammen slik at de har den fullstendige kompetansen."* [Informant 01]. Denne virksomheten viser at forståelsen for viktigheten av IKT-kompetanse på alle kompetanseområdene må være tilstede

for å oppnå kvalitet på bestillerkompetansen (NSM, 2018a). Her er det samsvar mellom praksis og teori. En annen informant sier *"Vi har fem års erfaring hvor vi har involvert mange og innhentet ekstern hjelp fra mange fagområdet. Vi har kjørt flere tjenesteutsettinger tjenesteutsettingen siden den gang og har opparbeidet oss mye erfaring på området."* [Informant 10]. Viseadministrerende direktør i en statlig virksomhet presiserer at de *"Har god bestillerkompetanse i dag. Er blitt vesentlig bedre og er nå ganske god fordi de besitter kompetanse på hva de må stille spørsmål om. Vi har fått på plass en del kompetanse som kan forstå markedet ved tjenesteutsetting. Det er ansatt egne ressurser som har jobbet med større tjenesteutsetting tidligere."* [Informant 06]. Disse virksomhetenes erfaringer viser at nettopp erfaring er en av de viktigste faktorene for å oppnå kunnskap om hvor viktig bestillerkompetanse er for en vellykket tjenesteutsetting med god kvalitet. Erfaring har gitt de kunnskap om viktigheten av tverrfaglig kunnskap for å oppnå kvalitet i kompetanseområdene (NSM, 2018a).

For en informant viser funnene at *"Det er todelt; det ene er den innkjøpstekniske bestillerkompetansen hvor det er høyt nivå. Den andre er den innholdsfaglige som beskriver behovet du ønsker å få løst. Det er en modningsreise for veldig mange ressurser hos oss. Spesielt ved beskrivelse av faglige behov slik at leverandørene forstår hva de skal løse. Det er behov for spisskompetanse for markedsforståelse som gjerne kunne vært bedre i enkelte tilfeller."* [Informant 07]. Som det påpekes må virksomheten utvikle tverrfaglig bestillerkompetanse for å oppnå kvalitet.

NSM anbefaler at bestillerkompetansen som minimum dekker virksomhets-, sikkerhets-, integrasjonskompetanse. Videre bør kompetanse om anskaffelser og juridisk kompetanse dekkes. (NSM, 2018a). Svært få henviser til at de innehar denne bestillerkompetansen. Alle informantene oppgir at dersom de ikke innehar bestillerkompetanse selv henter de den inn og/eller supplerer eksternt. Det er imidlertid slik at få nevner hvilke kompetanseområder som bør dekkes for å oppnå kvalitet (NSM, 2018a). Flere henviser til anskaffelseskompetanse, noe som kan bety at fokuset på å dekke de ulike kompetanseområdene med tilhørende IKT-kompetanse i bunn ikke er tilstede. En informant påpeker imidlertid at de ser behovet for tverrfaglig kompetanse *"Vi er veldig oppmerksomme på at bestillerkompetanse består av mange deler. Det styrende dokumentet gjør at de enkelte fagmiljøer ikke kan bestille noe uavhengig av bruk av tverrfaglige ressurser. Dette er bevisst, nettopp for at man vet at dette er så sammensatt"* [Informant 01]. Dette viser samsvar mellom anbefaling og praksis. En

fagdirektør presiserer at *"Det er liten eller ingen egenkompetanse på bestillerkompetanse i Staten. Dette ble skaffet gjennom innleie av konsulenter med stor og bred erfaring på anskaffelser og bestillerrollen. Bestiller kompetansen var stor. Det ble inngått store og kompliserte avtaler som er meget gunstige for staten. Tok ikke helt innover seg de store investeringene og de tunge brukerkravene som kom."* [Informant 08]. Denne uttalelsen viser at de forstod behovet for bestillerkompetanse og innhentet eksterne ressurser for å bidra til kvalitet på kompetanseområdene.

Videre oppgis det fra en Kvalitets- og sikkerhetsansvarlig at *"Skal man levere kvalitet må man ha tid og ressurser til å gjøre det, noe som mangler i dag."* [Informant 02]. Dette viser at virksomheten ikke har forstått viktigheten av bestillerkompetanse. Med bakgrunn i at disse har avsluttet en tjenesteavtale begrunnet med for dårlig kvalitet, er det oppsiktsvekkende at det ikke er tatt lærdom av jobben som ble gjort forrige gang. De bør ha større fokus på betydningen av god bestillerkompetanse og dens betydning for kvalitet på tjenesteutsettingen. (NSM, 2018a)

4.3 I hvilken grad gjennomføres risikovurdering?

Det er risiko forbundet med tjenesteutsetting, både når det gjelder prosessering til og lagring av informasjon, forvaltning, utvikling og drift av tjenesten. For å styre risiko må alle tiltak og aktiviteter vurderes og gjennomføres (Aven, Terje (2015). Ved tjenesteutsetting blir verdikjeden lenger og mer komplisert da kjeden forlenges med leverandører, samt at bruk av underleverandører gjerne er tilstede. I de tilfeller hvor tjenesten settes ut til utlandet må også landvurdering gjennomføres (NSM 2018b). Det er risiko knyttet til alle disse forholdene. For å ha kvalitet på styring og kontroll må disse forholdene risikovurderes, håndteres og akseptabelt risikonivå må settes. Dette følger av risikostyringsprosessen (NS-ISO 31000:2009). Risikovurderingene vil være en del av den helhetlige tilnærmingen til risikostyring (IIA Norge 2017). Den må gjennomføres for å finne riktig risikonivå, hvilke behov for tiltak av sikring som trengs og for å ta de riktige beslutningene (NSM 2018a). Disse momentene som del av risikovurdering må belyses, vurderes og være en del av risikovurderinger i forkant av at tjenestene settes ut til private aktører.

I hvilken grad har man helhetlig risikostyring (Enterprise Risk Management ERM)?

Helhetlig risikostyring er nært knyttet til virksomhetsstyring, forholdet mellom virksomheten mål og strategier, og hvordan risiko håndteres og knyttes til måloppnåelsen (IIANorge 2017)

(Coso). I all hovedsak sier informantene at dette er anbefalt, eller at det skal etableres en helhetlig risikostyring. Kun tre av ti oppgir at de har etablert system for helhetlig risikostyring. En av disse påpeker at *"Helhetlig risikostyring er godt dokumentert i styrende dokumenter for prosjekt og i porteføljedokumenter"* [Informant 01]. En annen sier *"Det ligger et dokumentert system over hvordan helhetlig risikostyring skal være og brukes"* [Informant 06]. Flere informanter oppgir at det er under etablering. De fleste henviser imidlertid til at de skal eller har rutiner for hvordan risikostyring skal foregå eller viser til at det er et punkt i deres sikkerhetspolicy. De anser det som momenter i en helhetlig risikostyring. Dette kan tyde på at modenheten på hva helhetlig risikostyring innebærer ikke er fullt ut tilstede hos de aller fleste (Sæther, Hans Solli 2016). Ingen henviser til risikobasert tilnærming eller konkrete metoder og prosesser knyttet til måloppnåelsen gjennomført av styre, ledelse og ansatte som ligger til grunn for helhetlig risikostyring, eller enterprise risk management (Coso). Slik sett oppnår ikke disse kvaliteten i den helhetlige risikostyringen. Over to tredjedeler av virksomhetene har ikke innført en egen systemløsning for å oppnå en helhetlig risikostyring. Målet med helhetlig risikostyring er å holde risiko på et ønsket nivå og sikre best mulig balanse mellom trusler og muligheter. I tråd med styrets, og toppledelsens, risikoappetitt og forretningsstrategi (IIA Norge 2017). Uten at det er innført eller innføres et eget system for helhetlig risikostyring vil det være vanskelig å oppnå nettopp dette. Det viser således en motstrid mellom teori og praksis.

I hvilken grad er det etablert metode og metodikk for risikovurdering?

Som en del av risikostyringsprosessen skal det gjennomføres risikovurderinger (NS-ISO 31000:2009). For å kunne gjennomføre risikovurderinger bør man ha etablert en metode som viser på hvilken måte, og med hvilken metodikk det skal gjennomføres. Slik kan man oppnå et rammeverk som stiller krav slik at det blir gjennomført planlagte og systematiske aktiviteter for å styre risikoene (IIA Norge 2017). Det er variasjon i om det er besluttet metode og krav til bruk av metode for å gjennomføre risikovurderinger. Enkelte har krav til det i policyer, men mangler en formalisert metode. Andre har det som krav gjennom internkontrollsystem. En viseadministrerende direktør forteller at det i ettertid av en uheldig hendelse har medført stor endring rundt risikovurdering og metodebruk. Vedkommende påpeker at *"Det er etablert og videreutviklet et system for risikovurdering. Dette er forankret i toppledelsen. Vi videreutvikler dette ytterligere. Det er videreutviklet mye i etterkant av uheldig tjenesteutsetting. Det kan synes som om at metodikken for risikovurdering ikke er fulgt ved den uheldig tjenesteutsettingen. Det er krav til risikovurdering i Kvalitetssystem fra 2010, og i*

Styringssystem for informasjonssikkerhet med eget risikovurderingsdel" [Informant 06]. Det viser at det har vært læring og utvikling av modenhet (Sæther, Hans Solli 2016) og forankring i ledelsen (IIA Norge 2017). I risikostyringsprosessen er det en forutsetning for å lykkes, at ledelsen er involvert (NS-ISO 31000:2009). I motsetning til dette funn uttaler en annen *"Det var ikke aktuelt å etablere metoder for risikovurdering med en nyopprettet organisasjon på det tidspunktet"* [Informant 08]. Det viser motstrid mellom teori og praksis. Flere bruker to-faktor med sannsynlighet og konsekvens som metode for å beskrive risiko. Andre synes det er mer hensiktsmessig å sette fokus på tilsiktede uønskede handlinger og benytter tre-faktor med verdi-, trussel- og sårbarhetsvurderinger til formålet. Funnene viser variasjon på om det er etablert og formalisert metode og metodikk, og bruken av to- eller tre-faktor modell.

Hvordan og i hvilken grad gjennomføring det risikovurderinger?

Risikovurderinger skal være gjennomført som en del av risikostyringsprosessen, og omfatter risikoidentifisering, risikoanalyse og risikoevaluering (NS-ISO 31000:2009). En forutsetning er at det gjennomføres gode risikovurderinger slik at det kan tas de riktige beslutninger (NSM 2018a). Det er nødvendig å gjennomføre risikovurderinger for å få identifisert risiko og for å få kartlagt sikkerhetsnivået. Man må ivareta både de organisatoriske, menneskelige og teknologiske forholdene for å få frem helheten ved gjennomføring av risikovurderinger. Den enkelte virksomhet har selv ansvar for å gjennomføre risikovurderinger med god kvalitet. Risikostyring fordrer planlagte og systematiske tiltak for å kunne styre risikoene. Dette kan best realiseres gjennom en risikovurdering.

For kommunal sektor oppgir informantene at det er besluttet at risikovurderinger skal gjennomføres, men at det er variabelt om det skjer basert på hvor i sektoren man anskaffer systemene fra, og hvilken type endring som utføres. Bakgrunnen for dette kan bero på manglende implementering og at det forårsaker variasjon. En informant forteller at de *"Forsøker å presse på for å få gjennomført risikovurderinger og har oppnådd en større oppmerksomhet rundt at dette er nødvendig. Det er besluttet at samtlige IT systemer som forvaltes skal gjennomgå risiko- og sårbarhetsvurderinger og eventuelt personvernkonsekvensvurderinger. Dette har ikke vært formalisert tidligere."* [Informant 02]. Dette viser til at det ikke er etablert noen formaliserte rammeverk, metodikk eller prosesser for hvordan risikovurderinger skal foregå (NS-ISO 31000:2009).

Når det gjelder statlig sektor viser funnene tilsvarende resultat med variasjon på når og hvordan risikovurderinger gjennomføres som kommunal sektor. Også her har de fleste vært besluttet gjennomført, men de mangler implementering. En viseadministrerende direktør oppgir at *"Tidligere er risikovurderinger gjennomført i noen sammenhenger, i andre ikke og det er flere mangelfulle risikovurderinger. Etter en uheldig tjenesteutsetting gjennomføres risikovurderinger i stort omfang."* [Informant 06]. Det at det nå gjennomføres risikovurderinger viser en økt modenhet (Sæther, Hans Solli 2016), samt at kvaliteten på risikostyringen ønskes bedret. En annen informant påpeker at *"Statlige system er tungrodd og det blir ikke satt opp for "spidd" i innføring. Vi hadde ikke tid til å vente på alle avklaringer. Dette er i stor grad tidsstyrt, det skulle bli ferdig. Det er veldig krevende i et statlig system med endringer hele tiden."* [Informant 08]. Denne virksomheten opplyser at det er laget en del risikovurderinger på deler av systemet for å finne ut hvor risikoen ligger. En service manager i statlig selskap forteller at *"Vi gjennomfører risikovurdering på flere nivåer, men det ble ikke gjennomført egen risikovurdering i forbindelse med fornying av tjenesteutsetting."* [Informant 10]. Dette er ikke i henhold til anbefalinger som gis om gjennomføring av risikovurderinger med riktig beslutningsgrunnlag for å oppnå god kvalitet (NSM 2018a). Funnene viser ingen forskjell på om risikovurderinger gjennomføres mellom statlige etater og statlige selskaper. Det er heller ingen synlige forskjeller på gjennomføring av risikovurderinger mellom statlig og kommunal sektor.

I hvilken grad vurderes tjenesteutsetting til utenlandske foretak?

Ved tjenesteutsetting i seg selv vil man få et høyere risikobilde. Når tjenesten settes ut til utlandet vil dette gi en enda lengre verdikjede. Slike kjeder blir enda mer komplekse og således fører de til en forhøyet risiko.

Når tjenesten vurderes satt ut til utlandet må landvurdering gjennomføres. Disse gjøres for å vurdere risiko knyttet til blant annet statlige styringsindikatorer, cybersikkerhetstilstanden, IKT infrastruktur og -kompetanse, og forretningsstabilitet. I denne vurderingen vil det være naturlig at man også vurderer verdiene og hvordan disse skal beskyttes. (NSM, 2018b).

Bevissthetsnivået av å sette tjenestene til utlandet og hvilken risiko det kan innebære er varierende. Daglig leder i kommunalt selskap presiserer *"Vi er gjennomgående skeptiske og ønsker en strategi på at det økonomiske ikke skal være førende. Behov for å styrke kompetansen på dette i alle ledd"* [Informant 03]. NSM Temarapport fokuserer på "*Ved*

tjenesteutsetting av IKT-tjenester til andre land bør en rekke forhold ved vertslandet vurderes fordi forholdene kan påvirke sikkerhetsrisikovurderingen" (NSM, 2018b s. 1). Tre av informantene forteller at de har krav til at tjenesteutsetting skal skje i Norge. To av disse er statlige aktører og et er et kommunalt selskap. En av deltagerne i undersøkelsen understreker at de ikke har *"[…] historikk på at utenlandske foretak blir risikovurdert"* [Informant 02]. Dette til tross for at de har trukket tilbake en uheldig tjenesteutsetting til utlandet. Kvalitets- og sikkerhetsansvarlig påpeker derfor at det er *"Planlagt at det i avtaleverk fremgår om utenlandske foretak benyttes. Skal i fremtiden inngå som et avklaringspunkt i anbud som skal legges ut"* [Informant 02]. Det viser modning å i ettertid vurdere risiko ved tjenesteutsetting til utlandet. En virksomhet har fokus på korrupsjon når de setter ut tjenestene til utlandet *"Med tanke på korrupsjon brukes den offisielle indeksen for korrupsjon og for hvitvasking: Basel."* [Informant 07]. Denne virksomheten har en god praksis som bekreftes av at det er et av momentene landvurderingen bør sette fokus på (NSM, 2018b).

Hvordan følges risikobildet opp?

Leverandøroppfølging er viktig for å kunne følge endringer i risikobildet over tid og for å kunne måle kvaliteten på leveransen. NSM Temarapport påpeker at risikoen må følges jevnlig og gjennom alle faser av tjenesteutsettingen, da trusselbildet kan endres over tid, nye sårbarheter kan oppstå og nye opplysninger om vertslandet eller leverandøren kan oppstå (NSM, 2018a).

Seks informanter oppgir at de har oppfølging av risikobildet. En av disse forteller *"Det er etablert en leverandørstyring innenfor for digitale IT miljøet hvor det er etablert en egen funksjon for oppfølging av risikobildet. Risikobildet blir fulgt opp i forhold til avtaler. Risikostyring er avhengig av risikobildet og hva slags avtaler som er inngått."* [Informant 01]. En annen informant forteller at *"Systematisk rapportering til ledelsen av risiko fra driftsleverandør og foretak hvor man følger med på utvikling og hvilken risiko man tar."* [Informant 06]. Denne virksomheten har tidligere hatt en uheldig tjenesteutsetting som ble stoppet og har deretter fått et økt fokus på risikoregime (Engen mfl. (2016)). De øvrige oppgir kun oppfølging av risiko på en begrenset del av leveransen. En av disse har hatt hovedfokus på tid og kostnad. Andre har overlatt oppfølging til de sikkerhetsansvarlige, mens daglig leder i et kommunalt selskap uttaler at det *"bør løftes opp til ledergrupper og på den måten unngå at enkeltpersoner blir sittende med risikoen. Regelmessige gjennomganger av risikobildet av helheten og de den daglige hendelse- og avvikshåndtering"* [Informant 03]. Dette er ikke

praksisen i virksomheten i dag, men intensjonen til å få det til er tilstede. Det betyr at en tredjedel av informantene oppgir et uklart bilde av om risiko reelt følges formalisert opp. Risikoregulering er en forutsetning for å kunne utføre egenkontroll og vil være en del av sikkerhetsstyringen på leveransen. Fire av informantene forteller at det gjøres lite eller ingenting for å følge opp risikobildet i dag. Det bør foreligge et reguleringsregime som leverandører følges opp på. For å kunne utøve internkontroll, det gjelder både lovpålagt myndighetskontroll og egenkontroll må det etableres et reguleringsregime som følger opp leveransen på risikobildet (Engen mfl., 2016). Det viser at det ikke er samsvar mellom teori og praksis.

4.4 I hvilken grad blir det stilt krav til IKT-tjenesten og leverandør?

IKT-anskaffelser som en faktor for forbedret IKT-sikkerhet kan være fornuftig. Bedre tilgjengelighet på tjenesten kan bidra til mer stabile og tilgjengelige tjenester (NOU 2018:14). De kan således være viktige tiltak for sikre og forbedre IKT infrastruktur og IKT løsninger. Det betyr at det er viktig å stille de riktige og relevante kravene til tjenesten. (NSM, 2018a) Man må være oppmerksom på hva slags risiko man tar og hvilke nye risikoer som oppstår som følge av en tjenesteutsetting. Tjenesteutsetting er ikke risikofritt og ved manglende bevissthet kan man risikere å ikke få frem alle typer risikoer. Det er avgjørende at man stiller riktige og kvalifiserte krav til anskaffelsen av tjenesteutsettingen. For å kunne gjøre dette må man ha god kompetanse og erfaring som kravstiller Den som skal stille kravene må være forberedt på hvordan kravene skal utformes og hvilken grad av detaljer man ønsker på de (Aven, 2015). Aven beskriver det på følgende måte *"Trenden i tiden er å bruke mer overordnede, funksjonelle krav som uttrykker hva vi ønsker å oppnå, fremfor å spesifisere nøyaktig hvilke løsninger som skal brukes"* (Aven, 2015, s 121).

Hvilke krav til leverandør av tjenesten blir stilt?

Det vil være flere type områder som må fremgå av et kravdokument ved anskaffelse. NSM Temarapport sier *"Det bør utarbeides et kravdokument for alle faser av tjenesteutsettingen, det vil si selve anskaffelsen, forvaltning og driftsfasen samt ved terminering av kontrakten"* (NSM, 2018a, s 17). Flere av informantene har fokusert på de ulike fasene ved tjenesteutsettingen, anskaffelsen, forvaltning og driftsfasen. For en av informantene har det vært viktig å påpeke at *"Hovedavtale med hovedleverandør med krav til tjenesten. Disse ble videreført til ny leverandør og overført en annen leverandør i 2012. Det ble opprettet underleverandører etter at kontrakt om endelig kontrakt ble inngått, vedtak ble gjort allerede*

i begynnelsen av 2011." [Informant 08]. Virksomheten hadde avtalt at de skulle varsles og godkjenne alle endringer av underleverandører. Dette opplevde de at ikke ble fulgt når endring av underleverandører ble foretatt. Dette ble oppdaget og fulgt opp fra den statligeetaten. Her er det samsvar mellom anbefaling om leverandøroppfølging og praksis. Enkelte av virksomhetene har kun fokusert på krav i forbindelse med anskaffelsen. Andre henviser kun til funksjonelle krav eller sikkerhetspolicy. Andre påpeker at de bruker etablerte generelle standarder, med henvisninger til disse som krav til IKT-tjenester. Funnene viser imidlertid at godkjenningsrutiner for underleverandører og deres bruk av underleverandører ikke har hatt særlig fokus. Terminering av kontrakt er det ingen av virksomhetene som har fokus på, dette til tross for at flere av virksomhetene har trukket tilbake og avsluttet tjenesteutsettinger til utlandet. Viseadministrerende direktør fra et statlig foretak oppgir: *"Det stilles sikkerhetskrav. Vi har laget noen rutiner for dette. Krav om at leverandør leverer risikovurderinger."* [Informant 06]. Det kan tyde på at de kun har krav om risikovurderinger og ikke særskilte krav for alle faser av tjenesteutsettingen. En teknoligdirektør uttaler at det er *"Varierende i forhold til hva som skal anskaffes, stilles både sikkerhetskrav og krav til tjenesten."* [Informant 05]. Dette viser avstand mellom teori og praksis.

Dersom en leverandør ikke kan levere på de krav som er stilt må virksomheten se på risikoen ved tjenesteutsettingen og hva det medfører. De må vurdere om dette innebærer behovet for kompenserende tiltak. (NSM, 2018a) Dette gjelder uavhengig av om tjenesten skal settes innenfor eller utenfor Norge.

I hvilken grad blir det stilt sikkerhetskrav til IKT-tjeneste og leverandør?

Det vil være naturlig å ta utgangspunkt i risiko og ytelse for å kunne angi hvilke barrierer som er nødvendig, og hvilken beredskap det må tas høyde for ved utarbeidelsen av sikkerhetskrav. De overordnede og funksjonelle kravene til sikkerhet bør ta utgangspunkt i størrelsene på risiko og ytelse (Aven, 2015). Det bør således være etablert et sett med sikkerhetskrav for anskaffelse. Dersom man for eksempel mangler et styringssystem for informasjonssikkerhet vil det være vanskelig å komme opp med de riktige sikkerhetskravene ved anskaffelse av tjenesteutsetting.

Det er variasjon i om og hvordan sikkerhetskrav stilles. Teknologidirektør i en kommune uttaler at "Avhengig av type tjeneste. Har ikke klassifisert enda, men er under utarbeidelse. Foreløpig i variende grad, mangler systematikk på området." [Informant 05]. En Service

manager hos statlig selskap oppgir at det ikke stilles sikkerhetskrav i dag, mens en annen henviser til minstekrav innenfor en sektor. For en av virksomhetene kan det tyde på at de overlater ansvaret for å holde seg innenfor sikkerhetskrav til leverandøren. Vedkommende påpeker at *"Vi kjenner ikke til om det følges noen standarder. Det er en sikkerhetsarkitektur som ligger i bunn og som driftsleverandøren har ansvar for å drifte og forvalte. Det er opp til kunden selv å bestemme på hvilket nivå i sikkerhetsarkitekturen de enkelte tjenester skal ligge."* [Informant 10]. En annen informant forteller at *"Det finnes et gammelt kravdokument som ikke nødvendigvis er kompatibelt i dag. Vil derfor forsøke å få leverandører til å svare tilfredsstillende på og i samsvar med NSM sine grunnprinsipper for IKT sikkerhet, norm for informasjonssikkerhet i helse- og omsorgssektoren, og andre relevante standarder i tillegg til lovgivning."* [Informant 02]. Dette viser mangel på praksis. Når det gjelder tre av informantene opplyser disse at de stiller tydelige sikkerhetskrav. Områdedirektør i kommunal organisasjon oppgir at det *"Stilles krav i henhold til den sikkerhetspolicy man har, gjelder både for leverandører og underleverandører. Gjelder helt ut i alle ledd. Har utarbeidet egne kravspesifikasjoner og en driftsavtale som regulerer kravene og det som skal dekkes. Alle forhold som skal følges opp er nedfelt i avtaler."* [Informant 04]. Den andre informanten forteller at *"Det stilles sikkerhetskrav. Blant annet personvernkrav og medisinsk teknisk utstyr og hvordan håndtere krav til anskaffelse."* [Informant 06]. En tredje, som har erfart at sikkerhetskrav ikke er fulgt opp av leverandør til tross for avtaleforpliktelse påpeker; *"Det er stilt krav i hovedkontrakten. Den er gjennomgått grundig på nytt. Dette har vært en stor læringsprosess som har kommet etterpå."* [Informant 08]. For disse viser det at det er samsvar mellom teori og praksis.

Som tidligere beskrevet sier Aven at trenden i dag ligger på overordnet nivå og i hva vi ønsker å oppnå, fremfor å spesifisere og ta det ned på et detaljert nivå. (Aven T., 2015). Ut fra de svarene informantene har gitt kan det se ut til at det er hold i det Aven legger frem.

4.5 Hvordan foretas beslutninger om tjenesteutsetting?

Beslutninger knyttes gjerne til dokumenter, blant annet en risikovurdering som beslutningsgrunnlag (Engen mfl., 2016). En beslutning om tjenesteutsetting bør bygge på det samme grunnlaget. Dette anbefales også av NSM, som anbefaler at beslutningsprosessene bør være godt forankret i organisasjonen. Beslutningen bør baseres på risikovurderinger som beskriver tjenesteutsettingens påvirkning på hele virksomheten og anbefales behandlet av øverste ledelse (NSM, 2018a). Ved tjenesteutsetting vil det være hensiktsmessig å benytte en

analytisk modell hvor *"man kan rangere alternativene etter deres konsekvenser, der man benytter en bestemt verdiskala eller målestokk"* (Engen mfl., 2016 s. 172). Dette harmonerer godt med å benytte risikovurdering som beslutningsgrunnlag. Faktorer som påvirker beslutningsunderlagets gjennomslagskraft vil avhenge av om det kan gi et klart råd eller om kompleksiteten i konsekvensbildet er slik at det representerer usikkerhet (Aven, 2015).

På hvilket nivå foretas beslutning om tjenesteutsetting i virksomheten?

Beslutningsnivå er hos åtte av ti virksomheter i ledelsen, mens det i noen tilfeller går helt opp til styret. Enkelte nevner at virksomhetens fullmakter og dets grenser for hva de kan signere legges til grunn, og følges ved anskaffelse av mindre kostnadskrevende tjenesteutsettinger. Dette er i henhold til god praksis. For de fleste virksomhetene synes det derfor at teori og praksis er godt avstemt. En informant forteller at beslutning om tjenesteutsetting fattes av tjenesteeier eller IKT-sjefen. Det kan antas at beslutningsgrunnlaget sees på uavhengig av hele virksomhetens mulighet for påvirkning (NSM, 2018a). Informanten med tilknytning til kommunal sektor uttrykker bekymring for at beslutningsgrunnlaget som fremlegges for ledelsen ikke godt nok, og at det kan inneholde usikkerhet som ikke blir kommunisert fordi det *"Blir besluttet i styre. Det virker som om beslutningsgrunnlaget ikke er godt nok gjennomarbeidet, at det ikke innehar nødvendige forhold og er kvalitetssikret i pågående tjenesteutsettelse."* [Informant 02].

Hvilke beslutningsprosesser følges?

En av risikofaktorene som vil påvirke beslutningsprosessene er *"Er beslutningsprosessen gjennomført og dokumentert i henhold til de relevante beslutningsprinsipper og – strategier?"* (Aven, 2015 s.153). Av funnene fremgår det at det både innenfor kommune- og statlig sektor har alle etablert beslutningsprosesser, men det er store variasjoner i hvem som involveres i prosessen og hvem som er beslutningstakere. Det er ingen forskjeller mellom kommunal og statlig sektor i behandlingen av beslutninger, verken på hvilket nivå i virksomheten beslutnigstaking tas eller på hvilke prosesser for beslutningstaking som følges. En av informantene forteller at *"Formaliserte beslutningsgrunnlag er etablert"* [Informant 03]. Områdedirektør i kommunal organisasjon forteller at *"Det er etablert en egen styringsmodell for beslutninger"* [Informant 04]. Funnene viser at kun to av ti har etablert beslutningprosesser som er i henhold til beslutningsprinsipper og –strategier. For disse to viser det at det er samsvar mellom teori og praksis for disse virksomhetene. For de øvrige

virksomhetene, til tross for at de fleste av disse har etablerte prosesser for beslutningstaking, følges prosessene allikevel ikke når beslutningser skal tas. Som nenvt tidligere er også beslutninggrunnlaget av veldig variarende kvalitet og stort sett ikke innenfor akseptablelt risikonivå. Til tross for at de fleste oppgir å ha etablerte prosesser for beslutningstaking viserfunnene at kun to av ti er innenfor anbefalinger om dokumenterte beslutningsprosesser i henhold til beslutningsprinsipper og –strategier (Aven, 2015 s.153).

NSM påpeker at en beslutning bør baseres på hvordan den påvirker hele virksomheten og at risikovurderingene skal gjenspeile dette (NSM, 2018a). En informant påpeker at det er en *"Egen prosedyre som innlemmer styret, foretak, regionale foretak, faggrupper og driftsleverandør før det går til styret. Bred involvering i hele systemet"* [Informant 06]. Dette er en viktig observasjon da det viser modning på beslutningsgrunnlaget. Disse har avsluttet en avtale om tjenesteutsetting med bakgrunn i blant annet manglende beslutningsgrunnlag fremlagt for toppledelse og styre. Her vises det en modning i hvem som bør involveres for et robust beslutninggrunnlag og hvem som er beslutningstakere. En annen av informantene forteller at *"Det er ikke forankret med nødvendig spisskompetanse. Perspektivet får i stor grad internt IT-fokus for den enkelte kommune og går glipp av kritiske perspektiver fra andre virksomhetsområder"* [Informant 02]. Her er det et motsetningsforhold mellom anbefaling og praksis.

Et av spørsmålene i problemstilling er hvilke risikofaktorer som veier tyngst i beslutningsprosesser. Kun en informant nevner at økonomi er en styrende faktor ved beslutningstaking. To informanter nevner at IKT-miljøet blir de styrende faktorene i beslutningsprosessene. De faktorene som er gjennomgående og som det kan tyde på veier tyngst i beslutningsprosessen, er å involvere ledelsen og i noen tilfeller styrer i beslutningsprosessen. Ingen har nevnt spesielle faktorer som leder frem til beslutningsprosessen som fremtredende faktorer for beslutningen. Det tyder på at det er godt forankret hos de fleste virksomhetene at ledelsen skal involveres i beslutningsprosessen.

Empiri delen er gjengitt fra de svarene informantene ga under intervju. I det videre vil empiriske funnene bli benyttet i drøftingsdelen.

5 Drøfting

I dette kapitlet vil det drøftes teoretiske perspektiver og hvordan disse samsvarer med de empiriske funnene i oppgaven. Deretter drøftes problemstillingen med hvilken kvalitet risiko representerer ved tjenesteutsetting i offentlig sektor. Kapitlet er delt inn i de fem temaene som ble presentert i metodekapittelet, og vil være strukturert etter disse. Spørsmålene fra intervjuguiden og empirien vil drøftes og fremgå som egne avsnitt under hvert tema de representerer.

5.1 Hvordan oppfatter informantene kvalitet på styring og kontroll ved tjenesteutsetting?

For styring er det nødvendig å skaffe kontroll over hele livsløpet til tjenesteutsettingen. Knyttet til denne oppgaven drøftes det i lys av styring og kontroll og det er derfor vektlagt forberedelser og forvaltning fra NSM Temarapport (NSM, 2018a). Det vil redegjøres for de teoretiske perspektivene knyttet opp mot problemstillingen, og deretter vil det vurderes hvordan dette er ivaretatt ved å se på de empiriske funnene for hvert av underspørsmålene.

Det første som bør være på plass ved en tjenesteutsetting er risikoregulering. Disse risikoreguleringene er nødvendige fordi man i samfunnet trenger reguleringsregimer som ivaretar en styringsrettslig (Engen mfl. 2016) ordning som regulerer de ulike saksområdene.

Disse risikoreguleringene er nødvendige fordi man i samfunnet trenger reguleringsregimer som ivaretar en styringsrettslig (Engen mfl., 2016) ordning som regulerer de ulike saksområdene. Norske myndigheter gir føringer og pålegg gjennom Stortingsmeldinger, NOU'er og i ulike strategier. I forbindelse tjenesteutsetting er det gitt føringer i Stortingsmelding (Meld St 38, 2016-2017) og NOU (NOU 2018:14) om at tjenesteutsetting er ønskelig. Andre myndighetsaktører som NSM påpeker i sine risikorapporter de ulike truslene for flere risikofaktorer ved tjenesteutsetting i sine risikovurderinger (NSM, 2019 a) (NSM, 2019b). Det fremgår anbefalinger for landvurdering il det i Temarapport for landvurdering (NSM, 2018b). Det bør derfor være etablert et styringssystem som regulerer hva som skal styre risikoen, og hvilke risikoelementer som bør være ivaretatt. Dette vil igjen gi grunnlag for å ivareta kvaliteten på tjenesteutsettingen. Dette er førende elementer uavhengig av hvilken standard eller hvilket rammeverk som legges til grunn for styringssystemet (NS-EN

ISO 31000:2009) (NS- ISO/IEC 27001:2013) (COSO ERM, 2017) (IIA Norge, 2017). Standard for ledelsessystemer for kvalitet - Krav påpeker viktigheten av å ha planlagte og gode forberedelser av kvalitetsarbeidet og etablere, implementere og vedlikeholde prosessene (NS-EN ISO 9001:2015). I NSM sin Temarapport under punktet om oversikt og kontroll på hele livsløpet (NSM, 2018a), vektlegges det at det er belyst at det gjøres forberedelser, samt hvilke vurderinger som er gjort i forkant av en tjenesteutsetting. De knytter dette opp mot en IKT-strategi, og om det er besluttet å ta i bruk tjenesteutsetting.

Sett hen til problemstillingens ene punkt *"På hvilken måte vurderer offentlig sektor risiko knyttet til tjenesteutsetting av digitale IKT tjenester?"* vil risikostyring være viktig for å styre risikoen. Standard for Risikostyring sitt punkt med iverksetting av risikostyring og risikostyringsprosessen er sentrale elementer for å styre risikoen (NS-EN ISO 31000:2009 s. 16). Det har ikke fremkommet noen informasjon fra informantene om at virksomhetene har etablert eller implementert dette. Det viser en tydelig avstand mellom anbefalte tiltak for styring av risiko og hvilken praksis man i dag finner i den offentlig sektor.

Generelt er det fremkommet svært lite informasjon om virksomhetene følger et risikoregime, om det er etablert et styringssystem og hvordan dette gjenspeiler de krav og føringer som kommer ved en tjenesteutsetting. Flere har henvist til at det er etablert et styringssystem etter standard for styringssystem for informasjonssikkerhet (NS- ISO/IEC 27001:2013) og at dette gir føringer om at risikovurdering skal gjennomføres. Helhetlig risikostyring hvor man koordinerer og styrier ulike risikoområder er vesentlig i risikostyringen (COSO ERM, 2017). Helhetlig risikostyring legger til grunn at det må være kommunikasjon mellom nivåene og prosessene, og må ha en forankring i mål og styring. Det er få som har etablert helhetlig risikostyringssystemer. Spesielt ved tjenesteutsetting hvor det er ulike hovedformål for å sette ut tjenesten vil det være viktig å ha systemer som ivaretar helheten og styrer risiko innenfor alle risikoområdene. Det fremstår som et misforhold mellom anbefalte styringsmekanismer og prosesser for å oppnå kontroll og få kvalitet på risikostyringen. Virksomhetene utøver således ikke god praksis for helhetlig risikostyring. Kun en virksomhet har henvist til et gammelt kvalitetssystem. Utover det er det ingen flere som har henvist til noen etablerte styringssystem for ledelsesystemer for kvalitet (NS-EN ISO 9001:2015), eller styringssystem for risikostyring – prinsipper og retningslinjer (NS-EN ISO 31000:2009). Både DFØ (DFØ, 2019a) og COSO (COSO ERM, 2017) påpeker at kvalitetsstyring er en strategisk beslutning

for å oppnå god styring og kontroll. Tilsvarende påpeker DFØ (DFØ, 2019a) og IIA Norge (IIA Norge, 2017) viktigheten av risikostyring.

De empiriske funnene ved hovedformålet med tjenesteutsettingen viser at flere henviser til at hovedformålet er å få prøve markedet, samt å få dekket det behovet de har gjennom skytjenester. Få eller ingen henviser til at det er en del av et strategisk valg med føringer gjennom mekanismer i de ulike styringssystemene. Det tyder på at behovet for modernisering og tilgang på ny teknologi er de førende elementene. For å få en vellykket tjenesteutsetting bør det være fokus på et tilsvarende eller høyere nivå på tjenestekvalitet og IKT- sikkerhet (NSM, 2018a s. 9). For å oppnå det bør det finnes klare føringer, en god strategi og et etablert styringssystem som legges til grunn slik at det ikke blir markedet og skytjenester i seg selv som blir førende.

Empiriske funn viser at forberedelser av tjenesteutsettingen i ingen eller liten grad blir gjennomført i det omfang som forventes gjennom teorien. Det fremkommer ikke av funnene om det arbeides i henhold til styringsprinsipper og god praksis ved tjenesteutsetting, eller at det som en del av forberedelsene er vurdert om tjenesten kan og burde tjenesteutsettes. De virksomhetene som har hatt uheldige tjenesteutsettinger har endret praksis. Disse påpeker at de i pågående og kommende tjenesteutsettinger vil gjøre forberedelser gjennom å etablere en strategi og et oppfølgingsregime. Det fremkommer imidlertid at flere gjennomfører risikovurderinger som forberedelse til tjenesteutsetting. Det er i henhold til god praksis og vil avdekke mulige risikofaktorer. Kvaliteten på risikovurderinger vil drøftes nærmere under kapittel for risikovurderinger. I noen tilfeller blir det også gjennomført konsekvensvurderinger for personvern. Det kan tyde på at bevisstheten og modenheten (Sæther, H. S., 2016) ikke er tilstede for hva som bør ivaretas i forkant knyttet til tjenesteutsetting, og risikoen det kan representere i arbeidet. Resultatet er her i samsvar med, og underbygges av, de funn som er avdekket i forskning på modenhet ved outsourcing. Denne forskningen viser til "at beslutning om sourcing initierer omfattende organisatoriske endringsprosesser" (Sæther, H. S., 2016), noe som igjen viser at man ikke ser konsekvensene av en tjenesteutsetting og den risikofaktoren en tjenesteutsetting kan representere når man ikke foretar forberedelser i forkant av tjenesteutsettingen. Praksisen er ikke i samsvar med god praksis, ei heller ikke i henhold til anbefalte forberedelser i teorien.

Teorien påpeker viktigheten av å ha planlagte og gode forberedelser av kvalitetsarbeid og etablere, implementere og vedlikeholde prosessene (NS-EN ISO 9001:2015). Når det kommer til etablerte prosesser er det flere som skal utarbeide styringsdokumentene hvor blant annet prosesser skal inngå. Flere mener de har gode prosesser på dette, til tross for at svært få har disse etablert og forankret i styringssystemet sitt.

Enkelte bemerker at fagmiljøer foretar tjenesteutsetting uten å følge prosesser, eller at de prosessene som benyttes ikke er godt nok gjennomtenkt. Dette medfører for dårlig beslutningsgrunnlag. Det er således ikke etablerte prosesser som følges gjennom hele eller deler av linjeorganisasjonen. Det kan se ut til at det er store variasjoner i om det finnes etablerte prosesser, om de er kjent for hele virksomheten og om de følges. Enkelte er godt i gang med å få dette etablert, mens andre ikke har begynt.

Når det gjelder prosesser for oppfølging og leverandørstyring etter tjenesteutsetting er det forskjeller på om dette er etablert. I den grad det er etablert, er det stort sett innenfor hendelse- og avvikshåndtering. Ingen av prosessene før, under, eller etter, synes å følge systematiske og planlagte prosesser for styring av tjenesten. Dette samsvarer ikke med god praksis. Teoretiske perspektiver (Engen mfl., 2016) tilsier at styringssystemer med prosesser for identifisering av risiko, risikostyring og risikovurderinger burde være etablert for å oppnå god kontroll, samt å ha styringsmekanismer gjennom etablerte prosesser for risikostyring (NS-EN ISO 31000:2009) (NS- ISO/IEC 27001:2013) for hele virksomheten. Det bør etableres et ønsket nivå for risiko. En slik risikostyring vil skape den balansen som etterstrebes ved å balansere mulighetsrommet på den ene siden og sikkerhet på den andre siden. Dette vil føre til en etablert risikostrategi og man vil kunne se helhetlig på risikoer som kan muliggjøre dette ved et etablert ERM system (IIA Norge, 2017). Flere ser behovet for bedre planlegging da dette ikke blir gjort, eller at det er store mangler i planleggingen av tjenesteutsetting. Dette samsvarer ikke med det som forventes av planlegging i et kvalitetssystem, hvor det å blant annet er viktig å "ta hensyn til relevante krav" for oppnå mål, samt å finne tiltak for å balansere mulighetsrommet og risiko (NS-EN ISO 9001:2015 s.13-14). Empiriske funn viser at virksomhetene bør tilstrebe et kvalitetssystem ved å få etablert, implementert, vedlikeholdt og kontinuerlig forbedre prosessene for risikostyring (NS-EN ISO 9001:2015). Når det gjelder modenhet fremgår det av empiriske funn at de som har tjenesteutsatt over en tid eller har hatt uheldige tjenesteutsettinger har oppnådd en større modenhet i arbeidet med styringssystem og prosesser enn de øvrige virksomhetene. Dette samsvarer godt med

modenhetsmodellen som forstås som historien og fremtiden (Sæther, H. S., 2016). Denne modellen kan hjelpe ledere til å finne hvilket nivå de befinner seg på i modenhet av prosesser knyttet til tjenesteutsetting. En forbedring av arbeidet med prosesser anses nødvendig for å få kontroll og styring av risiko og kvalitet inn i prosessene.

Når virksomheter skal tjenesteutsette, bør det sikres at man har tilstrekkelige kunnskap til å vurdere alle områder som blir berørt av det. Som en av informantene påpeker, er status for kunnskap om tjenesteutsetting at det "Handler i stor grad om manglende ressurser. Modenheten er lav, viljen er stor og evnen lavere". Med unntak av et par virksomheter, gir dette utsagnet en god beskrivelse, samt at det underbygger i stor grad funnene om kunnskapsnivået. De empiriske funnene viser videre at flere av virksomhetene innhenter sin kunnskap fra leverandører og konsulenter. Dette er ikke i overensstemmelse med anbefalinger om at man bør inneha kunnskap om tjenesteutsetting slik at man oppnår full styring og har kontroll på tjenesteutsettingen.

To av informantene opplyser at de har kvalitetskrav. En tredje forteller at virksomheten har noen krav knyttet til kvalitet av informasjonssikkerhet. Funnene viser at de øvrige ikke kan vise til noen konkrete kvalitetskrav. De empiriske funnene viser således at svært få stiller krav til kvalitet. Dette er i motstrid til standarden om Ledelsessystemer for kvalitet, og de krav den stiller (NS-EN ISO 9001:2015). I denne standarden forventes det blant annet at kvalitetspolicyen skal sikre en kontekst og at en strategisk retning i organisasjonene er forenlige (NS-EN ISO 9001:2015 s.12). Disse virksomhetene følger således ikke krav til kvalitet og det er i motstrid til forventningene til offentlig sektor, og hva som faktisk blir gjort. Dette har betydning i forbindelse med en tjenesteutsetting da det uten føringer på kvalitet kan bidra til at nivået på kvalitet vil være lavere enn det som ønskelig, og således vil dette påvirke kvaliteten på selve tjenesteutsettingen.

Leverandørstyring følges opp av alle, men hvordan og hva som følges opp er svært varierende. En informant påpeker følgende *"Nå er en del av strategien å sette ut leverandørstyringen til en integratorrådgiver. De skal lære opp organisasjonen i etterkant"*. Dette utsagnet viser liten modenhet i organisasjonen for leverandørstyring og er ikke i henhold til anbefalinger for god praksis. Flere informanter har opplyst at de har opplevd å måtte trekke tilbake kontrakter. En av informantene kunne også vise til kontraktsbrudd ved bruk av underleverandør som ikke var godkjent av kunden. NSM Temarapport (NSM, 2018a)

anbefaler at man har en plan dersom tjenesteutsettingen ikke går som planlagt. Ingen av informantene har nevnt om de har reflektert rundt, lagt planer for hvordan, eller om det er forberedt hva som skal skje ved kontraktsbrudd, endrede eller uakseptable forhold ved vertslandet og/eller leverandør. De har heller ikke nevnt tilbakeføring og/eller overføring og sletting og hvordan dette skal foregå. Bevissthetsnivået rundt dette synes å ikke være tilstede. De empiriske funnene viser at det ikke er overenstemmelse mellom praksisen funnene viser, og det teorien anbefaler. Funnene viser at viljen er tilstede etter den siste tids hendelser, samt at den siste tids hendelser har bekreftet viktigheten av kvalitet i tjenesteutsetting. Teorien legger til grunn at det finnes etablerte og planlagte prosesser og styringssystem. Den viser videre at ved å implementere kvalitetssystem, samt integrere det i etatens styringssystemer vil man få forbedret kvalitet i tjenesteutsettingen. Dette underbygges av det som fremkom i funnene og etatenes erkjennelse av nødvendigheten for å få etablert prosesser og styringssystemer for kvalitet til bruk ved tjenesteutsetting.

I forhold til problemstillingens spørsmål om offentlig sektor vurderer risiko knyttet til tjenesteutsetting av digitale IKT tjenester, og med hvilken kvalitet synes det ikke som det er kontroll på og at kvaliteten på risikostyringen er tilfredsstillende.

5.2 Hvordan oppfatter informantene kvalitet på bestillerkompetansen i virksomheten?

For å oppnå en vellykket tjenesteutsetting må virksomheten har god bestillerkompetanse slik at alle perspektiver og risikofaktorer blir ivaretatt (NSM, 2018a).

Engen mfl. påpeker dette når han tar opp egenskapene deltakende aktører må besitte for å bidra med innflytelse (Engen mfl., 2016). Videre presiserer Engen mfl. at "Jo mer en aktør har av inflytelsesressurser, jo større muligheter har han til å kunne påvirke beslutningsprosessen og resultatet." (Engen mfl., 2016 s. 178). Dersom bestillerkompetansen er svak kan resultatet bli at tjenesteutsettingen gjennomføres uten at det er vurdert hva som skal ivaretas gjennom livsløpet til tjenesteutsettingen. Alt fra forberedende aktiviteter til opphør av avtalen (NSM, 2018a). Avhengig av bestillerkompetansen virksomhetene innehar vil dette kunne påvirke risikoen knyttet til tjenesteutsetting.

NSM Temarapport (NSM, 2018a) og Engen mfl. (Engen mfl., 2016) anbefaler at man har bestillerkompetanse for å unngå at resultatet ikke innehar den kvaliteten den bør oppnå. NOU

Sikkerhet i alle ledd presiserer viktigheten av tilgang på kompetanse (NOU 2018:14). Funnene viser at det er store ulikheter i hva man oppfatter som god bestillerkompetanse og hvem som involveres utover IT-miljøet. Funnene viser at hos noen av virksomhetene er det mangelfull eller ingen bestillerkompetanse. Flere oppgir at de har bestillerkompetanse, men funnene viser likevel stor variasjon i hva de legger i begrepet.

For en av virksomhetene endte det med at avtalen opphørte. Det vektlegges i NSM Temarapport at anbefalingen er at virksomhetene besitter tverrfaglig bestillerkompetanse (NSM, 2018a). Det fordrer at virksomhetene bygger tverrfaglig egenkompetanse på bestillerrollen. Det interessante er at ingen av virksomheten trekker dette frem selv. De henviser til at de innehar kompetanse på enkelte fagområder og kan innhente ekstern faglig kompetanse. Ved innhenting av ekstern kompetanse kan resultatet bli at de eksterne ivaretar sine egne interesser fremfor virksomhetenes. Dette kan føre til manglende innspill om gode krav til IKT-tjenesten og et beslutningsgrunnlag som ikke representerer alle risikoområdene med tilhørende risikofaktorer. Det vil igjen gi et dårlig beslutningsgrunnlag for beslutningstagerne.
Grunnen til manglende bestillerkompetanse kan være flere, men det kan se ut fra funnene at det har vært for lite fokus på bestillerkompetanse. Funnene viser videre at dette nå er i bevegelse. Flere henviser til enkelt faggrupper som innehar kompetanse på bestillerrollen, men ingen oppgir at flere fagmiljøer samlet utgjør bestillerkompetansen. Dette er ikke samsvar med NSM Temarapport som belyser hvilken bestillerkompetanseressurser som bør involveres. Videre anbefales det at man "ivaretar behovet for bestillerkompetanse gjennom hele livsløpet til tjenesteutsettingen, og som et minimum har følgende kompetanseområder ved en tjenesteutsetting er virksomhets-, sikkerhets-, integrasjons-, anskaffelse- og juridisk kompetanse som blir benyttet ved tjenesteutsetting, og innehar disse funksjonene nødvendig grunnleggende IKT kompetanse" (NSM, 2018a). Denne totale bestillerkompetansen er det ingen av virksomhetene som har innehatt, men en av virksomhetene har etablert det i etterkant av en uheldig tjenesteutsetting.

De empiriske funnene viser at det for flere av virksomhetene ikke er samsvar mellom deres bestillerkompetanse og anbefalingene til NSM Temarapport. Det er ikke samsvar mellom praksis og teori. Virksomhetene burde ha identifisert hvilken kompetanse som var nødvendig og fått med seg den tverrfaglige kompetansen i vurderingene av risiko slik NSM Temarapport anbefaler (NSM, 2018a). God og tverrfaglig bestillerkompetanse vil gi god kvalitet på

beslutningsgrunnlaget og gitt beslutningstagerne det beslutningsgrunnlaget de trenger for å fatte riktig beslutning. De vil da få fremlagt relevante risikofaktorer som igjen gir oversikt over de organisatoriske, menneskelige og teknologiske risikoene knyttet til den konkrete tjenesteutsettingen, og således fatte en beslutning med bakgrunn i et akseptabelt risikonivå. Videre burde virksomhetene ha sett på hvem i de ulike fagmiljøene som bidrar slik at man bruker de ressursene som kan ha størst innflytelse på resultatet. Hvis dette hadde blitt gjort ville virksomhetene ha arbeidet i samsvar med de anbefalinger som Engen mfl. påpeker er viktig for å det beste resultatet for påvirkning på beslutningstaking (Engen mfl., 2016). Med hensyn til risiko knyttet til tjenesteutsetting, er det å inneha god og tverrfaglig bestillerkompetanse ikke tilstede hos de fleste av virksomhetene. Dette betyr at risikoen for manglende bestillerkompetanse utgjør en risiko knyttet til tjenesteutsettingen i offentlig sektor. Det at tverrfaglig bestillerkompetanse ikke finnes hos de fleste virksomhetene vil medføre at det for området bestillerkompetanse vil være en risiko for at ikke all risiko knyttet til de ulike risikoområdene er vurdert i henhold til god praksis (NSM, 2018a). Dette medfører at bestillerkompetansen blir en risikofaktor.

Bestillerkompetansen har ikke samsvar mellom den praksisen informantene oppgir virksomhetene har, og teorien for bestillerkompetanse og hvilken innflytelse deltakerne bør inneha tilsier (NSM, 2018a) (Engen mfl., 2016).

5.3 I hvilken grad vektlegges risikostyring og gjennomføres det risikovurderinger med god kvalitet?

Problemstillingen i oppgaven tar for seg hvordan risikovurderingene innvirker på kvaliteten av tjenesteutsettingen av digitale IKT tjenester. Det vil her drøftes hvordan risikovurderingene innvirker på kvaliteten av tjenesteutsetting av digitale IKT tjenester. Underliggende forskningsspørsmål er kritiske risikofaktorer knyttet til risikostyring. Det vil også drøftes hvordan risikofaktorer fra risikovurderingen innvirker på risikostyringen.

Risikovurderinger er et godt middel for å gi beslutningstaker godt beslutningsgrunnlag under forutsetning av at grunnlaget holder beslutningskvalitet. Risikovurderinger er en god beslutningsstøtte i arbeidet med å fatte beslutninger. Utfra et sett med risikokriterier vil man kunne gjøre tiltak, og gjennom det få et akseptabelt risikonivå. Den viktigste forutsetningen for at en risikoanalyse skal spille en viktig rolle i forbindelse med en beslutning, er at den har

kvalitet som gjør at *"grunnlaget for å kunne gjennomføre en god beslutning bør være tilstede"*. Risikobasert tilnærming vil bidra til å gi hjelp til å styre og å prioritere ressurser innen sikkerhet, og gi et beslutningsgrunnlag som kan dimensjonere sikringstiltak etter identifisert risiko. (Aven T., 2015).

Som en del av risikostyringsprosessen, anbefales det at det gjennomføres risikovurderinger (NS-EN ISO 31000:2009) (NS- ISO/IEC 27001:2013). Begge teoriene beskriver at risikovurderinger bør være planlagte og systematiske. Det betyr at virksomhetene bør ha etablert styringssystem med policyer, føringer og prosesser for risikostyring. Tjenesteutsetting bør være godt planlagt og føringer lagt i strategier for hvordan tjenesteutsetting skal foregå, slik at risikovurderingen kan vurdere risikoelementer i forhold til det. Det varierer om virksomhetene har etablert og besluttet metode og krav til risikovurderinger. Dette er i seg selv en risiko for de som ikke har dette på plass. Enkelte har krav i til gjennomføring av risikovurderinger, men mangler en formalisert metode, gir ulikt perspektiv på hvilke risikofaktorer som håndteres. Risikovurderinger vil dermed gjennomføres ulikt, og samme risikoelement blir behandlet og håndtert ulikt. Dette vil igjen skape ulikheter i forhold til risikoaksept, og beslutningsgrunnlaget som fremlegges for beslutningstakerne vil kunne veie akseptabelt risikonivå ulikt. Ved at det ikke er besluttede metoder og prosesser for hvordan risikovurderinger gjennomføres, vil skape usikkerhet om alle risikoelementer er ivaretatt, og om usikkerhet er vurdert. Dette er ikke i samsvar med anbefalte eller pålagte krav til å etablere rammeverk for risikostyring eller informasjonssikkerhet. Viktigheten av å gjennomføre risikovurderinger understrekes i NSM Temarapport som anbefaler *"gode risikovurderinger for å kunne ta riktig beslutning"* (NSM, 2018a). Virksomhetene gjennomfører i noen grad risikovurderinger. Kun enkelte har tatt i bruk risikostyringsprosesser. I kommunesektoren oppgir alle virksomhetene at de har krav til å gjennomføre risikovurderinger. De oppgir imidlertid at dette er avhengig av at flere forhold gjennomførers. For å få oversikt over risikobildet og eventuelt usikkerhet, er det helt nødvendig å gjennomføre risikovurderinger. Dette også for å få et underlag som skaper forutsigbarhet i beslutningsprosessen. Her er det motstrid mellom den praksis de har, og hva anbefalinger i teorien sier. (Aven T., 2015) (NSM, 2018a) (NS-EN ISO 31000:2009) (NS-ISO/IEC 27001:2013).

Risikostyringsprosessen (NS-EN ISO 31000:2009) hvor man setter kontekst, gjerne gjennom hvilke verdier man skal tjenesteutsette, for deretter å gjennomføre risikovurdering ved å identifisere, analysere og evaluere. Deretter risikohåndtere gjennom å sette tiltak, risikoaksept

og behandle risikovurderingen gir praksis i å gjennomføre risikovurderinger. Gjennom risikovurderingen vil man måtte se på trusler og sårbarheter og vurdere de opp mot verdien som skal tjenesteutsettes. Ved å bli kjent med verdiene, finne trusselbilde gjennom scenarioer, og få oversikt over sårbarheter, for deretter å finne risikoaksept og eventuelt sette på tiltak, vil gi et risikobilde av hvilke risikofaktorer som må hensyntas ved beslutning om tjenesteutsetting eller ikke. NSM gjennomfører flere risikovurderinger som vil gi innspill til hvilke risikoelementer man bør vurdere. Disse vil gi påvirkning på hvilke risikoelementer virksomheter i offentlig sektor bør ta høyde for i sine risikovurderinger av tjenesteutsetting av digitale IKT tjenester (NSM, 2019 a) (NSM, 2019b). I disse risikorapportene fremkommer flere generelle, men også helhetlig digitale risikofaktorer som bør knyttes mot tjenesteutsetting. NOU Sikkerhet i alle ledd understreker at "risikovurderingen må inngå som en del av en samlet vurdering av fordeler og ulemper som følger av tjenesteutsettingen". (NOU 2018:14 s. 59). I det videre drøftes risikofaktorer knyttet til risikovurderingene. Risikostyringsprosessen med gjennomføring av risikovurdering vil gi en god risikoforståelse og et godt beslutningsgrunnlag. Det er viktig at det her fremkommer et helhetlig bilde som igjen vil bidra til å skape risikoerkjennelsen. Ut fra dette, vil man kunne gi risikoaksept og sette det akseptable risikonivå og risikovurderingen vil være et godt verktøy for å gjøre dette for beslutningstagerne.

Teorien påpeker at man må ta hensyn der det er risikoelementer som fører til forhøyet risiko (Engen mfl., 2016). Dette presiseres også i NOU Sikkerhet i all ledd, og understreker at dersom det knytter seg forhøyet risiko til enkelte forhold, eller og at risikoen må reduseres til et akseptabelt risikonivå (NOU 2018:14 s. 59). Usikkerhet knyttet til risiko er et viktig risikoelement å få kontroll på (Engen mfl., 2016).

NOU Sikkerhet i alle ledd tar i rapporten opp tjenesteutsetting og påpeker "Tjenesteutsetting, inkludert bruk av skytjenester, er en betydningsfull trend som følge av digitaliseringen av samfunnet". Den følger opp med å si *"Gjennomgående fokuseres det på sikkerhetsrisikoer som, i henhold til fremstillingene, antas å ville oppstå fordi tjenesteutsetting foregår utenfor Norge."*. (NOU 2018:14 s. 59). Landrisiko er en risikofaktor som kan gi forhøyet risiko. Dette må tas hensyn til ved at risikovurderingen vurderer risikoelementene knyttet til landrisiko. NSM Temarapport anbefaler og gir veiledning på hvilke risikoer som knytter seg til, og bør vurderes i en landvurdering (NSM, 2018a) (NSM, 2018b). Funnene viser at i virksomhetene er det tre med krav til at tjenesteutsetting skal foregå i Norge, som gjør at dette ikke er relevant hos dem. Av de øvrige virksomhetene, er det en som vurderer korrupsjonsrate, den

andre oppgir at de vil ha et avklaringspunkt om tjenesteutsetting til utlandet i fremtidige anbud. Dette viser at det er stort forbedringspotensiale i å gjennomføre landvurdering ved tjenesteutsetting til utlandet. Dette er en risikofaktor som må belyses ved kommende tjenesteutsettinger til utlandet.

Det medfører risiko å ikke gjennomføre risikovurderinger. Risikofaktorer som vil påvirke tjenesteutsettingen vil da ikke vurderes. Uten en risikovurdering vil virksomhetene ha et manglende og svakt beslutningsgrunnlag. Det er ikke i henhold til anbefalinger. Virksomhetene er ikke tjent med å tjenesteutsette digitale IKT tjenester uten at risikobildet er kjent innenfor risikoaksept og innehar et akseptabelt risikonivå.

NSM Temarapport understreker i sin anbefaling at "Virksomheten må revidere risikoen knyttet til tjenesteutsettinger jevnlig, og gjennom alle faser av tjenesteutsettingen" (NSM, 2018a). Dette på bakgrunn av at risikobildet vil endre seg over tid. Når det gjelder oppfølging av risikobildet oppgir flere av virksomhetene at dette følges opp. Flere av disse har hatt uheldige tjensteutsettinger til utlandet, og har fått økt bevissthet på det. Det er bra og viser en modning i forhold til det å følge opp risikobildet. Det er imidlertid slik at nesten halvparten av virksomhetene oppgir at de kun følger opp i begrenset omfang. Et risikobilde som ikke følges opp i en digitaliseringsverden i rask endring, gir en risikofaktor som bør fokuseres på, og forbedres.

De kritiske risikofaktorer som er identifisert er å øke bestillerkompetansen, legge til grunn et bedre beslutningsgrunnlag basert på gode risikovurderinger, ved tjenesteutsetting til utlandet må landvurdering gjennomføres og det må etableres styringssystem som stiller krav til IKT-tjenesten.

5.4 Stilles det riktige og gode kvalitetskrav til IKT-tjenesten og leverandør?

Krav til IKT-tjenesten bør stilles for å den nødvendige oversikt over hvordan verdikjeden er og hvordan tjenesten skal implementeres? Spesielt viktig er dette ved tjenesteutsetting hvor verdikjeden blir lenger og mer komplisert. Det understrekes i NSM Temarapport at det er viktig *"For å finne gode krav må du kjenne sin egen virksomhet og vite hvilke behov du har."* (NSM, 2018a). Først da kan man stille krav gjennom en kravspesifikasjon om hvilke krav leverandøren skal ivareta. Disse må være i tråd med strategi og policy for tjenesteutsetting. Kravspesifikasjonen bør inneholde krav til sikkerhetsarkitekturen og informasjonssikkerhet. Det betyr at det må stilles krav til drift og utvikling for hvor informasjon lagres og prosesseres

fra, og hvor disse områdene har sin geografiske lokasjon (NSM, 2018a). Kun noen av virksomhetene stiller krav i forbindelse med selve anskaffelsen. Flere av informantene forteller at de bruker generelle standarder som krav til anskaffelsen. Disse har ikke gjennomført identifisering av sine egne behov knyttet til tjenesteutsettingen. Det er interessant at flere virksomheter innenfor offentlig sektor, noen av de med samfunnskritisk infrastruktur, ikke stiller krav til IKT-tjenesten. Ved å ikke strikke krav mister man en del av styringsmekanismene og kontrollen på tjenestene. Kun noen få av virksomhetene stiller i dag sikkerhetskrav. Dette er interessant sett opp mot at flere av de øvrige virksomhetene som ikke stiller disse kravene har tjenesteutsatt IKT-tjenester, også til utlandet.
En virksomhet henviser til NSM grunnprinsipper for IKT sikkerhet, men understreker at de skal få leverandøren til å svare om de er i samsvar med disse. Aven understreker at kravene til leverandørene bør settes mer overordnet og de funksjonelle kravene må gjengi ønsket måloppnåelse (Aven T., 2015). I Ledelsessystemer for kvalitet – Krav, henvises det til mange ulike krav for drift som vil gi mange detaljkrav. Dette viser i motstrid til teorien til Aven som presiserer at kravene til leverandørene bør bli mer overordnede.. Ingen av virksomhenete har oppgitt at de har etablert overordnede krav eller implementert det i kvalitetssystemet, men noen har henvist til at de stiller funksjonelle krav eller krav i henhold til sikkerhetspolicy. Det interessante her er at flere av virksomhetene har opplyst at de har etablert styringssystem for informasjonssikkerhet (NS- ISO/IEC 27001:2013). Det fremkommer ikke at de benytter dette bevisst i anskaffelsesprosessen ved tjenesteutsetting. Det kan gi store følger for samfunnskritisk infrastruktur, både økonomisk og omdømmemessig dersom man får ustabile tjenester eller brudd på informasjonssikkerhet og det er uklarheter knyttet til kontraktsforholdene om hvilke krav som er stilt til tjenesten. Ved å ikke stille krav etter behov eller inneha godkjenningsrutiner på leverandørsiden er ikke i overensstemmelse med de anbefalinger som gis. (NSM, 2018a) (Aven T., 2015) (NS-EN ISO 9001:2015).

Det at ingen av virksomhetene har fokus på terminering av kontrakter, er en interessant observasjon. Terminering av kontrakt og hvilke aktiviteter som skal utføres presiseres og anbefales i NSM Temarapport (NSM, 2018a). Ved terminering av kontrakt er det viktig å vite hvordan data skal håndteres, både hva angår "tilbakeføring, flytting og sletting av virksomhetens informasjon" (NSM, 2018a). Enkelte virksomheter i offentlig sektor har fått erfare hva det økonomiske og tap av omdømme kan koste. Det er et stort forbedringspotensial å få bevissthet på terminering av kontrakter ved tjenesteutsetting i offentlig sektor.

I forbindelse med tjenesteutsetting til utlandet er det viktig å foreta en landvurdering (NSM, 2018b). Flere av virksomhetene har satt ut tjenester til utlandet. Det fremkommer likevel ikke i funnene at de gjennomfører landvurdering med vurdering av landrisiko. Det er betenkelig at virksomhetene ikke i større grad er opptatt av det da flere av de har satt ut tjenester til utlandet. Det at det ikke gjennomføres landvurderinger ved tjenesteutsetting til utlandet er ikke i henhold til anbefalt praksis (NSM, 2018b) (NSM, 2018a).

NSM Temaveielder henviser til at minimumskravet til leverandør ved tjenesteutsetting blant annet bør være "Et etablert styringssystem for informasjonssikkerhet og sertifisering i henhold til internasjonale standarder, for eksempel ISO/IEC 27001:2017." (NSM, 2018b). Denne standarden eller 2013 utgaven av den og 27002 brukes av noen av virksomhetene. Flere av informantene henviser under styringssystem eller risikovurdering til at de har etablert styringssystem etter standard for Informasjonsteknologi (NS- ISO/IEC 27001:2013) (NS-ISO/IEC 27002:2013). De virksomhetene som har etablert styringssystem etter denne standarden har ikke nevnt om de stiller tilsvarende krav til leverandører ved tjenesteutsetting.

Ved tjenesteutsetting stilles det ikke alltid krav til IKT-tjenesten utgjør en risikofaktor ved tjenesteutsetting i offentlig sektor.

5.5 Fattes beslutninger på riktig nivå i virksomheten og med hvilken kvalitet på beslutningsgrunnlaget?

Beslutning om tjenesteutsetting bør bygge på et veldokumentert beslutningsgrunnlag. For å oppnå dette benyttes gjerne en risikovurdering (Engen mfl., 2016). Dette underbygges også av veileder for risikostyringsfunksjonen som påpeker at "Risikostyring og beslutninger henger sammen" (IIA Norge, 2017). De fremhever videre at det bør stilles krav til ulike scenarioer som et underlag til strategiske beslutninger (IIA Norge, 2017).

I NSM Temarapport poengteres det at *"Beslutningen om tjenesteutsetting bør ikke utelukkende tas av virksomhetens IKT-miljø alene. Valg av leverandørmodell og tjenesteutsetting av IKT-tjenester er en viktig strategisk del av virksomhetsstyringen. Virksomhetens leder bør sørge for en godt forankret prosess for alle berørte parter i virksomheten. Når en beslutning om tjenesteutsetting tas, bør den baseres på risikovurderinger som beskriver tjenesteutsettingens påvirkning på hele virksomheten, herunder leveranseevne, IKT-portefølje, økonomi og behov for kompetanse."* (NSM, 2018a

s.19). Funnene viser variasjoner i beslutningsprosessen for tjenesteutsetting, både på nivå og med hensyn til hvilke føringer som finnes for å danne et beslutningsgrunnlag. Det fremkommer at beslutningsnivået stort sett finnes hos ledelsen og hos enkelte anvendes styrebehandling. Dette er god praksis og i samsvar med teorier som anbefaler at beslutning om tjenesteutsetting behandles av øverste ledelse (NSM, 2018a).

Til tross for at de fleste virksomhetene oppgir at de har etablerte beslutningsprosesser, viser variasjonene i funn at det er forskjeller på hvordan beslutning om tjenesteutsetting fattes, og at funnene ikke er i overensstemmelse med teorien. Ut fra funnene er det vanskelig å påpeke noen konkrete årsakssammenhenger til forskjellig praksis for beslutning om tjenesteutsetting.

Aven diskuterer kompleksiteten i om konsekvensbildet representerer usikkerhet og at beslutningsunderlagets gjennomslagskraft vil avhenge av om det er økonomisk forsvarlig eller ikke (Aven T., 2015). En interessant observasjon er at kun en av informantene uttrykker bekymring for at beslutningsgrunnlaget ikke er godt nok og kan inneholde usikkerhet. Kun en av ti virksomheter tar altså opp spørsmålet om beslutningsgrunnlaget og dets kvalitet skaper en bekymring for at det ikke er nok fokus på det, samt hvilken usikkerhet det kan representere. Informantene blir under tema styring og kontroll forespurt om usikkerhet. Der oppgir de fleste at usikkerhet ikke blir kartlagt, og de gir uttrykk for at de ikke er kjent med om det innhentes informasjon om usikkerhet. NSM Temarapport påpeker at det antas at beslutningsgrunnlaget vurderes uavhengig av hele virksomhetens mulighet for påvirkning (NSM, 2018a). Kun et fåtall av informantene vurderer usikkerhet i forkant av eller gjennom risikovurdering. Dette vil bidra til at risikoelementer hvor usikkerhet ikke er kartlagt ikke kommer frem i beslutningsgrunnlaget.

Aven påpeker at "klarhet i beslutningskriterier er vesentlig for å kunne ta en god beslutning" (Aven T., 2015 s. 166). Risikovurderinger kan være et beslutningskriterie. Det fremkommer der at det er variasjon i om risikovurderinger gjennomføres, samt kvaliteten på dem. Betydningen av tydelige beslutningskriterier synes ikke å være tilstede. Her mangler det samsvar mellom teori og praksis. De fleste oppgir at det er besluttet gjennomført, men mangler implementering. Det betyr at i noen tilfeller legges risikovurderinger frem som beslutningsgrunnlag. Det finnes således i noen grad risikovurdering som beslutningsgrunnlag, men disse representerer stort sett ikke usikkerhet eller et helhetsbilde av risikofaktorer. Det betyr at alle vesentlige risikoer ikke kommer tydelig frem av beslutningsgrunnlaget.

Beslutningsgrunnlaget kan derfor mangle informasjon som kan være avgjørende for risikoaksept og akseptabelt risikonivå. Beslutningsgrunnlaget bør veie tungt i beslutningsprosessene. Praksisen hos informantene er ikke i henhold til teorigrunnlaget til Engen mfl. (Engen mfl., 2016), eller anbefalingene til NSM Temarapport (NSM, 2018a) og veileder for risikostyringsfunksjonen (IIA Norge, 2017) som bygger på at det må finnes et pålitelig beslutningsgrunnlag som grunnlag for strategiske beslutninger. Beslutningsgrunnlaget blir således avgjørende for hvor gode beslutninger, og med hvilken kunnskap beslutningene fattes. Det er heller ikke her samsvar mellom praksis og teori (Engen mfl., 2016) (Aven T., 2015) (NSM, 2018a) (IIA Norge, 2017).

I problemstillingen etterspørres hvilke kritiske risikofaktorer som knytter seg til risiko. Usikkerhet i beslutningsgrunnlaget vil være en kritisk risikofaktor. Kvaliteten på beslutningsgrunnlaget er ikke i henhold til anbefalinger fra teori, Temarapport eller veileder (Engen mfl., 2016) (Aven T., 2015) (NSM, 2018a) (IIA Norge, 2017).

Når det gjelder beslutningtaking fremkommer det at virksomhetene stort sett har etablerte beslutningsprosesser, men at beslutningsnivå varierer. Beslutningsgrunnlaget er svært varaibelt, og usikkerhet er stort sett ikke vurdert. Ingen har oppgitt at de legger til grunn beslutningskriterier. Det vises imidlertid til at det gjennomføres risikovurderinger som fremlegges som beslutningsgrunnlag.

De faktorene som veier tyngst i beslutningsprosessene fremkommer i liten grad av empirien. Kun en påpeker at økonomi er førende og det alene anses som en risikofaktor. I drøftingen fremgår det at mangler i beslutningsgrunnlag veier tungt i beslutningsprosesene. Mangel på kartlegging av usikkerhet og gjennom dette vanskeligheter med vurdering av risikoaksept. For dårlig beslutningsgrunnlag veier således tyngst i beslutningsprosessen.

6 Konklusjon

Tjenesteutsetting gir mange muligheter og kan gi store fordeler for offentlig sektor ved forbedret kvalitet og en større bevissthet på vurdering av risiko, hvilke risikofaktorer man bør ta hensyn til og sikring av de som ikke er innenfor ønsket risikoaksept. Det vil gi et beslutningsgrunnlag som gir et bevisst forhold til akseptabelt risikonivå. Bedre styring av tjenesteutsetting er nødvendig for å opprettholde kontroll ved tjenesteutsetting. Dette er essensielt for å kunne ha kontroll på tjenesteutsettingen av digitale IKT tjenester.

Offentlig sektor vurderer risiko knyttet til tjenesteutsetting av digitale IKT tjenester forskjellig. Få har etablert risikoregulering med strategier og policyer som er fastsatt i styringssystemer som grunnlag for vurderingen. Det gjennomføres delvis risikovurderinger, men kvaliteten på disse, både om det blir gjennomført og hvilke risikofaktorer som helhetlig blir vurdert er sterkt varierende. Kritiske risikofaktorer identifisert gjennom arbeidet med oppgaven er å øke bestillerkompetansen, legge til grunn et bedre beslutningsgrunnlag basert på gode risikovurderinger, landvurdering ved tjenesteutsetting til utlandet må gjennomføres og det må etableres et styringssystem som stiller krav til IKT-tjenesten.

Når det gjelder styring og kontroll har de fleste av intervjuede virksomheter manglende etablerte styringssystemer, både innenfor kvalitet, risiko og sikkerhet. I den grad styringssystem er etablert er det innenfor informasjonssikkerhet hvor flere riktignok også har en prosess for risikostyring. Det er lite fokus på å etablere strategi og policy for tjenesteutsetting og å implementere disse i styringssystemet. Det er behov for at virksomhetene skaffer seg egen intern kompetanse på tjenesteutsetting.

Empiriske funn drøftet mot teori for god praksis og anbefalinger viser at kvaliteten på vurdering av risiko og risikostyring ved tjenesteutsetting i offentlig sektor har et forbedringspotensial. Det viser også at det er behov for en bedret og økt modenhet i virksomhetene hva angår tjenesteutsetting generelt, og vurdering av risiko spesielt. Det vil gi et bedre grunnlag for vurdering av akseptabelt risikonivå ved tjenesteutsetting og gi mulighet for en bevisst beslutningstaking av risikoaksept. Generelt for empiri vil pålideligheten til de svarene som fremkommer og om andre vil komme til samme resultat bero på om man benytter de samme informantene, om samme tema belyses og om tilsvarende spørsmål blir stilt. Det må fastsettes styringsprinsipper, metode og føringer for at risikovurderinger skal

gjennomføres ved tjenesteutsetting. Dette må følges opp i virksomheten slik at det skjer kontinuerlig ved endringer. Det må etableres styringssystem, og krav til IKT-tjenesten må fremkomme av disse og benyttes ved tjenesteutsettingen.

Beslutningsgrunnlaget viser mangler som kan føre til at risiko ved tjenesteutsetting ikke blir håndtert. Kvalitet på beslutningsgrunnlaget generelt, og risikovurdering som beslutningsgrunnlag spesielt har potensiale til å bli grundigere, samt at det kan brukes til å legge usikkerhet til grunn. Gjennomføring av risikovurderinger som fast beslutningsgrunnlag og for alle tjenesteutsettinger har et klart forbedringspotensial. Det vil gi mulighet for et bevisst forhold til risiko og sikring, samt danne grunnlag for risikoaksept. Kvaliteten på arbeidet med risikovurderinger og beslutningsgrunnlag bør forbedres.

For å oppnå akseptabel kvalitet og samtidig oppnå en helhetlig og bærekraftig tjenesteutsetting er det behov for endring i de fleste virksomhetene i offentlig sektor som er intervjuet i denne oppgaven. Unntaket er et par statlige selskaper som har tjenesteutsatt over tid, og et foretak som har tatt lærdom av en uheldig tjenesteutsetting. Flere av disse har erkjent dette under intervjuene. Funnene i oppgaven viser og beskriver behov for etablering og implementering av styringssystem med strategi og policy for tjenesteutsetting, og prosesser for vurdering av risiko. Det anses å foreligge et behov for forbedringsarbeid i vurderingen av risiko ved tjenesteutsetting i offentlig sektor, slik at det oppnås styring ved tjenesteutsetting og dermed oppnås kontroll på de digitale IKT tjenesteutsettinger.

På bakgrunn av funn i oppgaven anbefales det at de virksomhetene som ikke har etablert og implementert styringssystem med strategi og policy for tjenesteutsetting, og prosesser for risikostyring og -vurdering av risiko får det på plass. Det anbefales å få implementert strategi og policy for tjenesteutsetting slik at virksomhetene oppnår forbedret kvalitet og styring av risiko ved tjenesteutsetting.

Det finnes mange styringssystemer, standarder og rammeverk utover de det er referert til i oppgaven som kunne vært relevante. I tillegg finnes det tilknyttede mulige teorier fra standarder benyttet til risiko og kvalitetsoppnåelse av det, som ikke er belyst i oppgaven. Flere av disse kan være overlappende og/eller gitt tilsvarende kontroll på styring. Oppgaven har ikke mulighet til å favne alt. En del relevante ISO-standarder og norske standarder som ville ha innehatt kvalitet og/eller risikostyring som deler av oppgaven har berørt har dermed ikke fått plass. Disse er dermed valgt bort grunnet omfanget oppgaven kan ha, men kunne

også fint ha vært benyttet, se avgrensede metoder og verktøy. Teorivalg er gjort utfra en betraktning av hvilke som har størst relevans i forhold til dets nære tilknytning til kvalitet, risiko og risikostyring. Grunnet svar fra informanter på styring og kontroll, hvor besvarelsene stort sett har pekt på styringssystem for informasjonssikkerhet, er det valgt å ta med også sikkerhetsstyringsdimensjonen inn i oppgaven.

Råd, risikovurderinger, håndbøker, tema-hefter og veiledninger som kan ha relasjon til oppgaven fra Politiets sikkerhetstjeneste PST, Etterretningstjenesten og E-tjenesten er i all hovedsak ikke tatt inn i oppgaven. Nasjonal sikkerhetsmyndighet NSM sine Temarapporter "Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – en utdyping av området "beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet" (NSM, 2018a) og *"Anbefaling om landvurdering ved tjenesteutsetting"* (NSM, 2018b), og Risiko 2019 (NSM, 2019 a) og Helhetlig digitalt risikobilde 2019 (NSM, 2019b) har har dannet grunnlag for tilnærming og tema i oppgaven. NOU, Temarapporter og veiledninger for digital-, generell sikkerhet og informasjonssikkerhet som kunne vært relevante, men ikke er tatt med er blant annet NOU 2018:14 Sikkerhet i alle ledd og Nasjonal strategi for digital sikkerhet. Denne er kun benyttet i mindre omfang i oppgaven. Tilsvarende gjelder for området Personvern, og General Data Protection Regulation (Personvernforordning), og lover og forskrifter tilknyttet temaet kvalitet, risiko og tilstøtende fagtema tilknyttet dette er ikke tatt inn oppgaven.

De empiriske funnene viser at det er behov for å få etablert prosesser og styringssystemer for kvalitet til bruk ved tjenesteutsetting. Videre viser de at virksomhetene stort sett har behov for å etablere strategi for tjenesteutsetting som denne kan styres etter. Det viser også et behov for å implementere kvalitetssystem og integrere det i etatens styringssystemer. På denne måten vil man få forbedret kvalitet i tjenesteutsettingen. Det er ikke overenstemmelse mellom den praksis som funnene viser og det teorien anbefaler. De fleste viser imidlertid et ønske om, og viljen er tilstede for, forbedringer. Ikke minst skyldes dette hos flere egne, uheldige tjenesteutsettinger som har bekreftet behovet for større kvalitet. og risikostyring.

Med bakgrunn i de empiriske funn som er gjort i denne oppgaven er det behov for forskning på tjenesteutsetting i offentlige virksomheter, både med tanke på kvalitet, vurdering av risiko og risikostyring. Det anses også behov for å forske på de elementene ved tjenesteutsetting denne oppgaven ikke omhandler som økonomi, og Helse, Miljø og Sikkerhetsfunksjoner i et globalt, nasjonalt eller organisatorisk perspektiv.

7 Referanser

Aven, T. (2015): *Risikostyring*. (2. utg.). Universitetsforlaget

Blakie (2010): *Designing Sosial Research* (2. utg.). Cambridge: Polity Press.

COSO Enterprise Risk Management (2017) Hentet fra: https://iia.no/cosos-nye-rammeverk-for-risikostyring-enterprise-risk-management-integrating-with-strategy-and-performance/

Direktoratet for økonomistyring (2019) Kvalitetssystemer Hentet fra: https://dfo.no/fagomrader/internkontroll/internkontroll-i-etatsstyringen

Direktoratet for økonomistyring (2019a) *Kvalitetssystemer* Hentet fra: https://dfo.no/fagomrader/internkontroll/internkontroll-i-staten

Direktoratet for økonomistyring (2019b) *Kvalitetssystemer* Hentet fra: https://dfo.no/fagomrader/internkontroll/sammenhengen-kvalitet-og-internkontroll

Direktoratet for økonomistyring (2019c) *Kvalitetssystemer* Hentet fra: https://dfo.no/filer/Fagområder/Internkontroll/Veileder-internkontroll.pdf

Direktoratet for økonomistyring (2019d) *Risikostyring* Hentet fra: https://dfo.no/fagomrader/risikostyring/kravene-til-risikostyring-i-staten

Direktoratet for IKT og forvaltning (2019) *Internkontroll/Styringssystem* (versjon 1.4) Hentet fra: https://internkontroll-infosikkerhet.difi.no/begrepsliste#Risikostyring

Engen O.A.H., Kruke B.I., Lindøe P.H. Olsen K.H, Olsen O.E, Pettersen K.A. (2016): *Perspektiver på samfunnssikkerhet.* Cappelen Damm AS

Hood, C., Tothstein, H. og Baldwin, R. (2001) *The government of risk. Understanding regulation regimes*. Oxford, Storbritania: Oxford University Press.

International Organization for Standardization (ISO) (2009): SN-ISO Guide 73:2009. Standard Norge

International Organization for Standardization (ISO) (2015): NS-EN ISO 9000:2015 *Ledelsessystemer for kvalitet - Grunntrekk og terminologi*. Standard Norge

International Organization for Standardization (ISO) (2008): *NS-EN ISO 9001:2008 Ledelsessystemer for kvalitet Krav.* Standard Norge

International Organization for Standardization (ISO) (2015): *NS-EN ISO 9001:2015 Ledelsessystemer for kvalitet Krav.* Standard Norge

International Organization for Standardization (ISO) (2000): *NS-EN ISO 9004:2018 Kvalitetsledelse - Kvaliteten i en organisasjon - Veiledning til å oppnå vedvarende suksess,* Standard Norge

International Organization for Standardization (ISO) (2013): *NS-ISO/IEC 27001:2013 Ledelsessystemer Informasjonsteknikker Ledelsessystemer for informasjonssikkerhet Krav.* Standard Norge

International Organization for Standardization (ISO) (2017): *ISO/IEC 27001:2017 Information technology - Security techniques - Information security management systems - Requirements.* Standard Norge

International Organization for Standardization (ISO) (2013): *NS-ISO/IEC 27002:2013 Informasjonsteknologi Sikringsteknikker Tiltak for informasjonssikkerhet.* Standard Norge

International Organization for Standardization (ISO) (2015): *NS-EN ISO 31000:2009 Risikostyring Prinsipper og retningslinjer*, Standard Norge

Justis- og beredskapsdepartementet. (2016–2017) *IKT-sikkerhet* (Stortingsmelding Meld. St. 38 Melding til Stortinget). Tilråding fra Justis- og beredskapsdepartementet 9. juni 2017, godkjent i statsråd samme dag. (Regjeringen Solberg) Hentet fra: https://www.regjeringen.no/contentassets/39c6a2fe89974d0dae95cd5af0808052/no/pdfs/stm201620170038000dddpdfs.pdf

Nasjonal sikkerhetsmyndighet NSM (2018a) (versjonsnummer 1.1): *"Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – en utdyping av området "beslutt leveransemodell" i NSMs grunnprinsipper for IKT-sikkerhet".* Nasjonal sikkerhetsmyndighet Hentet fra:

https://www.nsm.stat.no/globalassets/dokumenter/temahefter/tjenesteutsetting2018v1.1_enkelstsider.pdf

Nasjonal sikkerhetsmyndighet NSM (2018b): *"Anbefaling om landvurdering ved tjenesteutsetting"*. Nasjonal sikkerhetsmyndighet Hentet fra: https://www.nsm.stat.no/globalassets/dokumenter/temahefter/anbefaling-om-landvurdering-ved-tjenesteutsetting.pdf

Nasjonal sikkerhetsmyndighet NSM (2019a): *Risiko 2019*. Nasjonal sikkerhetsmyndighet Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2019_final_enkeltside.pdf

Nasjonal sikkerhetsmyndighet NSM (2019b): *Helhetlig digitalt risikobilde 2019.* Nasjonal sikkerhetsmyndighet

Hentet fra: https://www.nsm.stat.no/globalassets/rapporter/2019---nsm-helhetlig-digitalt-risikobilde.pdf

Norges interne revisjonesforening IIA Norge (2017): *Veileder for risikostyringstyringfunksjonen Enterprise Risk Management (ERM),* IIA Norge Nettverk risikostyring Hentet fra: https://iia.no/risikostyring/nyheter/veileder-for-risikostyringsfunksjonen/

NOU 2018: 14 (2018) *IKT-sikkerhet i alle ledd Organisering og regulering av nasjonal IKT-sikkerhet*, Holte, Hans Christian med flere Hentet fra: https://www.regjeringen.no/contentassets/0d408600df2f4738a9bbb85040b02b59/no/pdfs/nou201820180014000dddpdfs.pdf

Røyksund M. (Mai 2018) Forelesingfoiler: *Risikoregulering*. Universitetet i Stavanger

Standard Norge (2019) *Standarder,* Standard Norge Hentet fra: https://www.standard.no/nettbutikk/sokeresultater/?search=beskrivelse+risikostyring

Sæther, Hans Solli (2016), *Modenhet i outsourcing, offshoring og backsourcing: Tilbake til fremtiden.* Professor ved NTNU Ålesund. *Magma*,19(2016)3:48-56 Hentet fra: https://biopen.bi.no/bi-xmlui/bitstream/handle/11250/2389301/Solli%20Saether_Magma%200316.pdf?sequence=1&isAllowed=y

7.1 Figurer

7.2 Tabeller:

7.3 Litteratursøk

Ved søk på tidligere tilsvarende studier finner man

- Risikovurderinger i forbindelse med outsourcing av informasjons- og kommunikasjonsteknologi (IKT) i petroliumssektoren UiS Ertenstein, Sissel; Løfgren, Silje Alvesen. Masteroppgave, Universitet i Stavanger, Vår 2018 (brage.bibsys.no)
- BORTE BRA, HJEMME BEST? Påvirker ulik organisering av brukerstøtte, brukernes tilfredshet med tjenesten? Wisløff, Annette. Master thesis, University of Oslo, 2014
- Cybersikkerhet Digitale sårbarheter i totalforsvaret, Masteroppgave i statsvitenskap, institutt for statsvitenskap, UNIVERSITETET I OSLO, Vår 2018 Lien, Christian
- MASTEROPPGAVE I YRKESPEDAGOGIKK Mai 2016 Ja takk begge deler – ikke enten eller. En oppgave om fagutdanning og yrkesidentitet Unni Hestsveen Fakultet for lærerutdanning og internasjonale studier, Institutt for yrkesfaglærerutdanning

Avgrensning standarder til teoridel

NS-EN ISO/IEC 27002:2017 Informasjonsteknologi - Sikringsteknikker - Tiltak for informasjonssikring

ISO/IEC 27005:2018 — Information technology — Security techniques — Information security risk management,

ISO/IEC 27017:2015 Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services,
ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,

NS 5814:2008 Krav til risikovurderinger- lagt til i referanseliste og vurderer henvise til i teori
NS 5830:2012 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi,
NS 5831:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse,
NS 5832:2014 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.

8 Vedlegg

1. Forespørsel til informanter
2. Intervjuguide

1. Forespørsel om å være informanter

Mitt navn er Anne Marie Dalen Øverhaug. Jeg er i ferd med å ferdigstille studie i master Risikostyring og Sikkerhetsledelse ved Universitetet i Stavanger og holder på med skriving av masteroppgave

Er offentlig sektor forberedt - Null eller full kontroll?
En studie på kvalitet på risikostyring ved digital/IKT tjenesteutsetting i offentlig sektor

I den forbindelse ønsker jeg å få anledning til et intervju med deg om hvordan kvalitet i risikostyringen ved tjenesteutsetting av det digitale/IKT miljøet foregår i din virksomhet. Til dette trenger jeg informanterenes hjelp til å identifisere situasjonen. I den forbindelse ønskes det å få intervjue deg om forholdene i din virksomhet.

Tidspunkt for intervjuet foreslås til
xxxdag xx.xx.xxxx Kl. xx.xx i deres lokaler.

Målet med oppgaven er å finne ut av hvilken kvalitet i risikostyringen som ligger til grunn i forkant av og ved en tjensteutsetting av digitale/IKT innen offentlig sektor. Gjennom intervju innenfor offentlig sektor ønskes det å belyse denne problemstillingen nærmere.

Spørsmålene er utformet i forhold til god praksis for kvalitet på risikostyringen. Det er viktig å få frem hvilken praksis som har eksistert tidligere og om hendelsene som har fremkommet den siste tiden har bidratt til endret praksis.

Håper du har anledning til å bidra til å få besvart hva som ligger til grunn av kvalitet ved risikostyringen ved digitale/IKT tjenesteutsetting. Håper foreslått tidspunkt passer for deg.

På forhånd takk for hjelpen.

Hamar, xx.xx.2019

Med vennlig hilsen

Anne Marie Dalen Øverhaug

2. Intervjuguide – spørsmål

Intervjuguide

Kvalitet i risikostyring ved digital/IKT tjenesteutsetting

INTERVJUSPØRSMÅL

1. **Styring og kontroll**

Hva har vært hovedformålet med den digitale/IKT tjenesteutsettingen?

Hvilke forberedelser gjennomføres i forkant av tjenesteutsetting?

Hvilke prosesser gjennomfører virksomheten før, under og etter tjenesteutsetting?

Hvilket kunnskapsnivå har virksomheten og hva ble utført av kunnskapsinnhenting i virksomheten i forkant av tjenesteutsetting?

Blir det kartlagt hvilken usikkerhet som tjenesteutsettingen representerer?

Hvilke kvalitetskrav benytter virksomheten ved tjenesteutsetting?

Hvordan følges leverandørstyring opp?

2. **Bestillerkompetanse**

Hvilken bestillerkompetanse har virksomheten?

Hvordan går virksomheten frem for å sikre seg riktig bestillerkompetanse og hvem involveres?

3. **Risikostyring og –vurderinger**

Har virksomheten etablert et eget system (rammeverk) og er det implementert bruk av systemløsning for helhetlig risikostyring (ERM)?

Hvilken metode og eller/metodikk for risikovurdering er benyttet og skal benyttes fremover?

Er og blir det gjennomført risikovurderinger?

Hvordan blir risiko ved tjenesteutsetting til utenlandske foretak vurdert?

Hva gjøres for å følge opp risikobildet?

4. **Krav til IKT-tjenesten og leverandør**

   Hvilke krav blir stilt til leverandør av tjenesten?

   Hvilke sikkerhetskrav blir stilt til IKT-tjeneste og leverandør?

5. **Beslutning om tjenesteutsetting**

   På hvilket nivå i virksomheten blir beslutningen om tjenesteutsetting fattet?

   Hvilke prosesser er fulgt for beslutninger?