DET TEKNISK-NATURVITENSKAPELIGE FAKULTET

MASTEROPPGAVE

Studieprogram/spesialisering: Risk analysis med spesialisering i risk governance

Vårsemesteret, 2022

Åpen / ~~Konfidensiell~~

Forfatter: Christian Sundfær og Hans Tore Haagensen

Fagansvarlig: Roger Flage

Veileder(e): Ruth Østgaard Skotnes

Tittel på masteroppgaven: Norske kommuners håndtering av risiko for cyberangrep via leverandørers IKT systemer

Engelsk tittel: Norwegian municipalities risk management of cyber-attacks through suppliers ICT systems

Studiepoeng: 30

Emneord: Risiko, cybersikkerhet, informasjonssikkerhet og anskaffelser

Sidetall: 133

+ vedlegg/annet: 3

Stavanger, 06.07.2022

Sammendrag

Denne oppgaven har sett på "hvordan norske kommuner jobber med risikoen for cyberangrep via leverandørers IKT-tjenester" og i forlengelse hvilke krav de stiller til leverandørkjeden, både gjennom interne prosesser, som oppdragsgiver og hva som ligger innenfor regelverket for offentlige anskaffelser. Til slutt har oppgaven også sett på hvordan kommuner opplever myndighetenes arbeid på området.

Vi som forfattere valgte tidlig å splitte teorikapittelet opp i flere deler. Risiko, informasjonssikkerhet, cybersikkerhet og anskaffelser. Denne delingen er gjort for å dekke det nødvendige spekteret for å svare ut det brede forskingsspørsmålet.

Ettersom som vi har benyttet oss av spørsmålsformen «hvordan» i denne forskningen og har hatt et ønske om å studere enkelthendelser, gå i dybden, belyse små detaljer og gi informanter frihet til å uttrykke seg er kvalitativ forskningsmetode med intervjuer brukt. Totalt sett har oppgaven 14 informanter spredt over flere kommuner, en interkommunal samarbeidsvirksomhet (IKS), Kommune-CSIRT og Orange Cyberdefence.

Vårt hovedfunn i denne oppgaven viser at kommunene er til dels beviste på risikoen for cyberangrep via leverandørkjedene og jobber aktivt med å redusere denne. Pr dags dato ligger kommunene i denne oppgaven i det nedre sjiktet av modenhetsgrad når det gjelder risiko, men basert på langsiktige planer er de i ferd med å implementere et bedre styringssystem med felles definisjoner, metodikk og forståelse for hvordan de skal arbeide med fagområdet. Videre har vi gjennom denne oppgaven funn som tilsier at kommunene med fordel kunne integrert et bedre sett med standardkrav til cyber- og informasjonssikkerhet i sine anskaffelser. Til slutt ønsker vi å trekke frem oppgavens funn hvor kommunene opplever at det er for mange myndighetsaktører på fagområdene, som i forlengelse benytter ulike tilnærminger slik at det blir uoversiktlig for de kommunale virksomhetene å identifisere anbefalt beste praksis.

Abstract

This thesis has looked at “how Norwegian municipalities work with the risk of cyber attacks via suppliers' ICT services” and, by extension, what requirements they place on the supply chain, both through internal processes, as a client and what is within the regulations for public procurement. Finally, the thesis has also looked at how the municipalities experience the authorities' work in the area.

We as authors chose early on to split the theory chapter into several parts. Risk, information security, cybersecurity, and procurement. This division is made to cover the necessary spectrum to answer the broad research question.

As we have used the question form "how" in this research and have had a desire to study individual events, go in depth, shed light on small details and give informants freedom to express themselves, qualitative research method with interviews is used. In total, the thesis has 14 informants spread over several municipalities, an inter-municipal cooperation, Kommune-CSIRT and Orange Cyberdefence.

Our main finding in this thesis shows that the municipalities are partly aware of the risk of cyber attacks via the supply chains and are actively working to reduce it. As of today, the municipalities in this thesis, are in the lower tier of maturity when it comes to risk, but based on long-term plans, they are in the process of implementing a better management system with common definitions, methodology and understanding of how to work with the subject area. Furthermore, through this thesis we have found findings that indicate that the municipalities could with advantage integrate a better set of standard requirements for cyber and information security in their procurements. Finally, we want to highlight the thesis' findings where the municipalities experience that there are too many government actors within the subject area, who by extension use different approaches so that it becomes confusing for the municipalities to identify recommended best practice.

Innholdsfortegnelse

Forord

Denne masteroppgaven er et resultat av det to-årige masterprogrammet "Risk analysis" med spesialisering innenfor "risk analysis and governance".

Gjennom denne oppgaven har vi jobbet med akademisk metode og egen definert problemstilling. Vi har fått muligheten til å utvikle kunnskapen vår ytterligere, etablert nye holdninger og utfordret de gamle hvor det har vært nødvendig. Læringskurven og arbeidsmengden har enkelte steder vært bratte, men også svært givende. I sum sitter vi igjen med et reflektert syn på fagfeltene risiko, cybersikkerhet og anskaffelser samt hvordan disse praktiseres i kommunalsektor for å motvirke leverandørkjedeangrep.

Det er en rekke mennesker som fortjener en takk i forbindelse med denne oppgaven. Først ønsker vi å takke de ansatte ved universitetet i Stavanger for å ha tatt oss gjennom denne kunnskapsreisen, videre ønsker vi å takke våre samboere for å ha støttet oss på hjemmebane underveis i hele studieløpet, vi takker også alle intervjuobjektene i oppgaven for deres kunnskapsdeling.

Til slutt retter vi en spesiell takk til vår veileder, førsteamanuensis Ruth Østgaard Skotnes. Gjennom sistnevntes positive innstilling og evne til å gi detaljerte tilbakemeldinger har oppgaven hevet seg over tid.

Tusen takk.

Christian Sundfær og Hans Tore Haagensen

06.07.22, Stavanger

Figuroversikt

Tabelloversikt

1 Innledning

«NSM observerer også at virksomheter lengre nede i verdikjedene rammes av sikkerhetstruende virksomhet, enten som mål i seg selv eller som ledd i å nå mål høyere opp i verdikjedene. Angrep som rammer leverandørkjeder er en økende risiko. Trusselaktørene kan for eksempel utnytte programvare- og tjenesteleverandører for å få innpass i systemene til selskapets kunder. Det er derfor viktig at virksomheter kartlegger sin plass i verdikjeden(e) og jevnlig vurderer egne avhengigheter.» (NSM, 2021c, s. 22)

Vi lever i en moderne verden i stadig utvikling og endring. Det moderne samfunnet tar i bruk ny teknologi i cyberdomenet for å effektivisere og skape nyvinning i et tøft marked. Både myndigheter, samfunnsfunksjoner og den enkelte borgeren er avhengig av den nåværende teknologien for å kunne kommunisere effektivt, delta i arbeidsprosesser og opprettholde tilgang til informasjon. Vi sender meldinger, filer, bilder og e-poster som aldri før, og forventer at hjelpemidlene skal utføre disse oppgavene umiddelbart, til enhver tid. Mange av de systemene vi bruker i hverdagen er avhengig av hverandre og internett og den stadige digitaliseringen vil bistå virksomhetene med enklere drift, bedre mobilitet, økt produktivitet og mer automatisert sikkerhet, men på den andre siden vil digitaliseringen gi økte digitale verdikjeder med komplekse systemer og større risiko som fører med seg avhengigheter og sårbarheter og leverandørkjeder representerer sårbarhetsflater for cyberangrep (NSM, 2022b; NSM, 2020b, s. 3).

«Et angrep mot en liten, lokal leverandør kan i ytterste konsekvens sette et globalt konsern ut av spill.» (NorSIS, 2021b, s. 15).

De siste årene har fokuset på sikkerhet i cyberdomenet økt drastisk, men mange henger etter og små og mellomstore bedrifter (SMB) er spesielt sårbare grunnet mangel på kompetanse, ressurser nok til å investere i sikrere systemer, samt egen leverandørkjede med usikker risiko (NorSIS, 2020, s. 7). Virksomheter i denne størrelsesorden har et spesielt fokus hos myndighetene for å ivareta god sikkerhet innad i leverandørkjedene ettersom disse bedriftene i veldig mange tilfeller er underleverandører til norske kommuner. Offentlig sektor blir derfor skiltet som et område som innehar størst risiko for leverandørkjedeangrep.

Cyberdomenet utvikler seg raskt, noe som skaper både nye muligheter og trusler. Selv om noen systemer kan fungere autonomt til tross for at de er tilknyttet de systemene som blir angrepet, er andre helt avhengige av sine samarbeidssystemer. Relasjonen i en leverandørkjede som både kan være sivile-militære eller offentlig-privat, fører til et dynamisk

trusselbilde som endrer seg i takt med utviklingen av ny teknologi og samfunnet i sin helhet. Trusler i og fra cyberdomenet kan slå ut viktige funksjoner som har mulighet for å gjøre store utslag på flere nivåer i samfunnet. Hendelsene vil være vanskelige å analysere på grunn av kompleksiteten og dermed skape et enda større tidspress på aktørene som skal utføre krisehåndteringen i første fase.

1.1 Oppgavens mål og forskningsspørsmål

Denne oppgaven har som hovedmål å se på hvordan norske kommuner jobber med risikohåndtering for cyberangrep via leverandørers IKT-tjenester og hvilke krav kommunene stiller til leverandørkjeden, både gjennom interne prosesser, som oppdragsgiver og hva som ligger innenfor regelverket for offentlige anskaffelser.

I tillegg ønsker vi å se på hvordan aktører som aktivt jobber med risiko for slike angrep har en bistandsrolle mot norske kommuners arbeid. Hovedtyngden vil ligge på kommunenes risiko og konteksten, teorien og datainnhentingen vil derfor fokusere mest på dette gjennom et søkelys på kommuners arbeidsform, rutiner og metodikk for å unngå leverandørkjedeangrep, samt hvordan de opplever samspillet med myndighetene.

Temaet og forskningsområdet er noe begge prosjektmedlemmene finner interessesant, både fordi vi ønsker å belyse sårbarheten som oppstår dersom IKT-sikkerheten innad leverandørkjedene er for svake og fordi temaet cybersikkerhet er noe vi begge brenner for og ønsker å ha som en profesjonell karriere fremover.

Cybersikkerhet er et tema vi mener må høyere opp i diskusjonene, både på samfunns-, organisasjons- og individnivå, for å skape en god og realistisk bevisstgjøring, slik at virksomheters og privatpersoners data sikres slik at vi opprettholder drift.

På bakgrunn av dette presenterer vi følgende problemstilling:

- **Hvordan håndterer norske kommuner risikoen for cyberangrep via leverandørers IKT tjenester?**

For å besvare hovedproblem stillingen vår bruker vi følgende forskningsspørsmål:

- **Hvordan implementerer norske kommuner risiko og cybersikkerhet i anskaffelser?**
- **Hvordan opplever norske kommuner myndighetenes arbeid med risiko og cybersikkerhet?**

1.2 Avgrensning

I denne masteroppgaven ser vi hovedsakelig på hvordan mellomstore kommuner (25 – 35 000 innbyggere) jobber med risiko for cyberangrep gjennom gode anskaffelser og kravstilling i deres leverandørkjeder, samt hvordan de opplever myndighetenes arbeid innen risiko og cybersikkerhet. Vi har hovedtyngde på kommunene med understøttende vinklinger fra faglige eksperter.

Risikoaspekter innen kommunaldrift via leverandørkjeder som økonomi og generell helse, miljø og sikkerhet (HMS) vil ikke være en del av undersøkelsen, men vil bli nevnt som henvisninger til årsaker eller eksempler. Det samme gjelder kommunal helhetlig risiko- og sårbarhetsanalyse (HROS) og hendelseshåndtering i form av krise- og beredskapsapparatet.

1.3 Tidligere forskning

Det finnes mye forskning innen tjenesteutsetting generelt, dette på bakgrunn av at det er et fenomen som har pågått lenge og stadig flere virksomheter tjenesteutsetter nye områder av sitt virke (Damanpour et al., 2019) og i Norge er det i størst grad innen finans og ledelse ved tjenesteutsetting forskningen har handlet om (Gottschalk, 2005a; Gottschalk, 2005b), men dette er overførbart til all type tjenesteutsetting. I tillegg belyser tidligere forskning risikoer ved fenomenet omstendelig og flere risikoer som følge av digitalisering over tid uavhengig hvilket område som skal tjenesteutsettes ettersom leverandører også i økende grad digitaliseres (Pettersen, 2018). I de tilfeller hvor forskning rundt digitalisering møter forskning rundt juridiske forhold med etterlevelse av krav i henhold til lovverk, vil det ikke være direkte overførbart, men heller ses på som en viktig faktor som må tilpasses norsk lovverk (Schartum, 2021).

Tjenesteutsetting gjøres i hovedsak på bakgrunn av globalisering og mye av forskningen understreker fordelene som tjenesteutsettingen medfører, deriblant finnes motivatorene som tilgang til kompetanse, fokus på kjerneaktiviteter, kostnadseffektivitet og økende konkurranse som ofte gjør at virksomheter tjenesteutsetter (Dhillon et al., 2017). Dog viser forskningen til en mengde risikofaktorer knyttet til tjenesteutsetting (Ibid; Fan et al., 2012), og det har ved flere anledninger blitt utviklet ulike modeller for risikovurdering og/eller rammeverk for å identifisere og håndtere risikoen (König & Spinler, 2016; Abdullah & Verner, 2012; Perlekar & Thakkar, 2018). En av de største utfordringene ved tjenesteutsetting er likevel risikovurderinger, spesielt på grunn av at informasjonssikkerhet har blitt en større risiko det er vanskelig å ha kontroll på, både grunnet kompleksiteten i systemene, men også under

oppfølgingen av tjenesteleverandør over tid (Fan et al., 2012; Khalfan, 2004). Håndteringen av risikoen er også utfordrende innen informasjonssikkerhet da eksisterende modeller anses å ikke treffe godt nok på de risikoelementene som er relevante og det er gjort flere forsøk på å utarbeide modeller og rammeverk for risikostyring innen dette feltet (van der Haar & von Solms, 2003; Nicho, 2018; Feng & Li, 2011). Informasjonssikkerheten trues av risikoer innen ulike kategorier fra teknologiske til organisatoriske som utgjør en større helhetlig risiko hvor konfidensialitet, integritet og tilgjengelighet er noe av det mest kritiske en må ivareta ved tjenesteutsetting (Dhillon et al., 2017; Al-Safwani et al., 2018).

Selv om den tidligere forskningen ikke direkte kan overføres vår problemstilling, vil mye kunne benyttes som et kunnskapsgrunnlag for tjenenesteutsetting opp mot risiko for leverandørkjedeangrep.

1.4 Sentrale begreper

Før vi går dypere inn i denne avhandlingen har vi valgt å legge en rekke sentrale begreper til grunn for besvarelsen.

Risiko

Risiko kan defineres som en eller en kombinasjon av flere faktorer som truer dagens eller ønsket situasjon (Renn, 2008, s. 1). Man kan også velge å se på risiko som en metode for å belyse avvik, ulykker og hendelser som truer ønsket måloppnåelse eller tilstand (Lupton, 2013, s. 3).

Risikostyring

Risikostyring kan defineres som «alle tiltak og aktiviteter som gjøres for å styre risiko. Risikostyring handler på den ene siden om å få innsikt i risikoforhold, effekt av tiltak, grad av styrbarhet av risiko osv., og på den andre siden metoder, prosesser og strategier for å kunne kartlegge og styre risikoene» (Aven, 2015, s.13).

Risikohåndtering

Risikohåndtering er en aktivitet som resultat av vurderinger av risiko. Aktiviteten tar i all hovedsak for seg å identifisere, velge og etablere tiltak for å motvirke risiko (Digdir, u.å.).

Trusler

En trussel er enhver handling (hendelse, omstendighet) som kan forstyrre, skade, ødelegge eller på annen måte påvirke en verdi negativt (og dermed en organisasjons virksomhet og drift). I et informasjonssikkerhetsperspektiv kan vi si at dette dreier seg ofte om hendelser som kan påvirke konfidensialitet, integritet og konfidensialitet (NOU 2015:13, s. 32).

Trusselaktør
For at trusler skal materialisere seg er en avhengig av en aktør som har evne, vilje og handlingsrom til å utsette en virksomhet for en ondsinnet handling. En trusselaktør drives av ulike motivasjoner og kan for eksempel variere mellom: enkeltkriminelle, hacktivister, organiserte kriminelle, kontraktører, statlige aktører osv. Det skilles ofte mellom avanserte og ikke avanserte trusselaktører basert på hvor stor evnen til aktøren er (Telenor, u.å.)

IKT
Informasjons- og kommunikasjonsteknologi (IKT) omfatter et vidt spekter av produkter med den fellesnevner om at de er basert på teknologi for elektronisk lagring eller overføring av informasjon. Nye tjenester og produkter gir til stadighet en økt samhandling på tvers av virksomheter (Mahieu, 2001).

Leverandører/underleverandører
En leverandør er en person eller virksomhet som har påtatt seg å yte eller utføre en leveranse av varer til en annen (Kaurel, 2020).

Leverandørkjede/verdikjede
En leverandørkjede utgjøres av de aktørene som er involvert utover egen virksomhet i fremstillingen av en vare, tjeneste eller produkt (Barne- og likestillingsdepartementet, 2009, s. 8).

Cyberdomenet
Cyberdomenet er et nettverk av teknologiske sammenkoblinger. Koblingene går gjennom både fysiske og logiske installasjoner eller informasjonssystemer. Eksempler på dette er kommunikasjonsinfrastruktur, media og data (Sundlisæter, 2013).

Informasjonssikkerhet
Informasjonssikkerhet innebærer å sikre informasjonsverdienes konfidensialitet, integritet og tilgjengelighet. Det er nødvendig å se tekniske tiltak i sammenheng med menneskelige og organisatoriske for å oppnå tilfredsstillende sikkerhet (Maal, Krogedal & Gjengstø, 2020).

Informasjonssystem
Nasjonal sikkerhetsmyndighet definerer informasjonssystemer som maskinvare, programvare og tilknyttet infrastruktur som i sum utfører oppgaver tilknyttet innsamling, lagring og behandling av ulike informasjonstyper. Mennesker interagerer og bruker informasjonssystemer for å støtte opp under egne eller virksomhetens prosesser for å oppnå målsetninger (NSM, 2020b).

Skytjenester
Skytjenester er en felles betegnelse på alt fra prosessering og lagring av data til programvare på servere tilgjengeliggjort fra eksterne serverparker gjennom internett (Datatilsynet, 2018a).

IKT-risiko
I forbindelse med risiko tilknyttet IKT er det flere definisjoner å jobbe ut fra, eksempelvis via NS 5832:2014. Her blir IKT-risiko omtalt som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen», også kalt trefaktormodellen (NSM, 2021b, s. 4).

Cybersikkerhet/IKT-sikkerhet/Digital sikkerhet
Cybersikkerhet er bredt begrep og brukes ofte synonymt med IKT-sikkerhet og digital sikkerhet, som tar for seg aktive grep for å beskytte og opprettholde sikkerdrift samt handlefrihet i cyberdomenet, enten du er en enkelt person, gruppe, organisasjon eller nasjon. Regjeringen definerte digital sikkerhet som: beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi (NOU 2015:13, s. 34).

Personvern
Datatilsynets beskrivelse av personvern fra 2018 legges til grunn i denne oppgaven. Personvern i norsk sammenheng innebærer både vernet av privatlivets fred og den enkeltes personlige integritet samt vernet av individers rett til innflytelse. (Datatilsynet, 2019a).

Cyberangrep
Cyberangrep er en aksjon utført av interne eller eksterne trusselaktører hvor hensikten er å påføre målet skade eller tap. Enten det er å ta ned systemer, uthente informasjon osv. Mål kan både være privatpersoner, grupper og virksomheter (Telenor, u.å.).

Offensiv nettverksoperasjon
I 2010 definerte Koordineringsgruppen for IKT –risikobildet, NSM, PST og E-tjenesten, offensive nettverksoperasjoner som utførelsen av én eller flere av følgende aktiviteter mot en annen virksomhet; 1) rekognosering, 2) infiltrasjon, 3) implantering, 4) informasjons-innhenting, 5) ødeleggelse, skadepåføring, disrupsjon eller nektelse, og 6) villedning. (NSM, PST & Etterretningstjenesten, 2010)

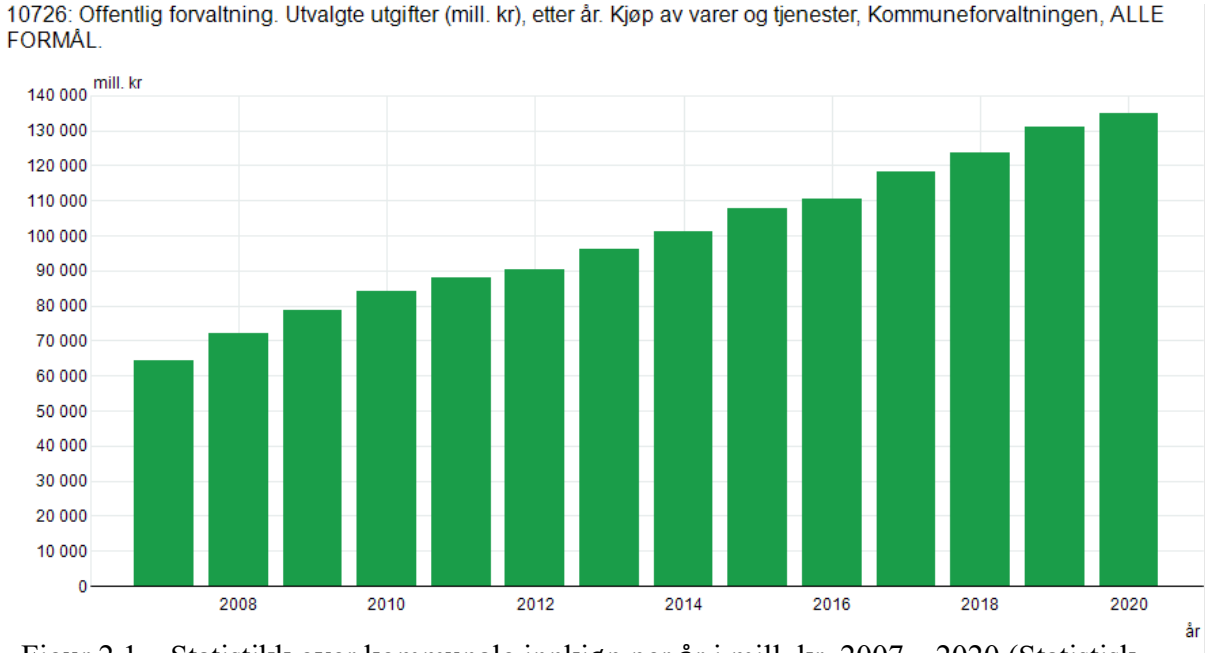
Kritisk infrastruktur
Kritisk infrastruktur er anlegg og systemer som er nødvendige for å opprettholde samfunnets kjerne eller kritiske funksjoner, (NOU 2006:6, s 32)

2 Kontekst og aktualisering

Offentlige virksomheter, spesielt kommuner, utkontrakterer stadig mer av sine tjenester til eksterne leverandører. Kristiansen (2015, s. 385) definerer tjenesteutsetting som:

«Begrepet utkontraktering kan i vid forstand defineres som tjenesteutsetting eller konkurranseutsetting, og innebærer at et foretak går over til å skaffe en vare eller tjeneste fra en ekstern leverandør, i stedet for å produsere eller levere denne selv»

Det foreligger en generell bekymring for at vurdering av sikkerhetsrisiko og etablering av sikringstiltak ikke får prioritet ved tjenesteutsetting, og spesielt ikke i anskaffelsens første fase (NSM, 2018a). Selv om leverandørkjedene innen offentlige anskaffelser begrenses til maksimalt to (Anskaffelsesforskriften, 2016, §19-2), og noen kommuner legger krav til kun ett ledd i leverandørkjeden (Oslo kommune, u.å), vil det fortsatt være ett til to ledd som en kommune må ha kontroll på i hver vertikalkjede, noe som blir mange å forholde seg til ettersom dette er per anskaffelse/ tjenesteutsetting og det gjøres flere og flere, og dyrere og dyrere anskaffelser over tid, noe som betyr at det blir flere og flere leverandørkjeder over tid å forholde seg til (se figur 2.1):



Figur 2.1 – Statistikk over kommunale innkjøp per år i mill. kr. 2007 – 2020 (Statistisk sentralbyrå, 10726).

Ved en gjennomgang av kommunenes offentlige tilgjengelige kravlister viser at det stilles lite eller få krav til leverandørene når det gjelder sikkerhet i cyberdomenet (Harstad kommune, u.å.; Os kommune, u.å.; Hol kommune, u.å.; Bamble-, Drangedal-, Kragerø, Porsgrunn-,

Siljan og Skien kommune, u.å.; Sarpsborg kommune, 2017) da dette ikke er et lovmessig forankret foruten noen styrende punkter rundt sikkerhet i kommunikasjonsmidler i anbuds- og anskaffelsesprosessen for å sikre fortrolighet og pålitelighet (Anskaffelsesforskriften, 2016, §22), samt andre bestemmelser innen personopplysningsloven (2018, art. 32-1) hvor det stilles noen ved vurderingen om behandlingens art, formål og omfang i lys av teknisk utvikling om at *«behandlingsansvarlige og databehandleren skal gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen»*.

2.1 Digitalt trusselbilde

Angrep på leverandørkjeder er ikke et nytt fenomen, men det som bekymrer er at dette er en stadig økende trend og Nasjonal sikkerhetsmyndighet (NSM) har de siste 7 årene hatt fokus på digital sårbarhet i leverandørkjeder fra deres første «Helhetlige IKT-risikobilde» i 2015 med henvisning til leverandørkjedeangrep i 2014 (NSM, 2015, s. 18) til siste risikoutgivelse (NSM, 2022b). Politiets sikkerhetstjeneste (PST) skriver i sin 2022 utgave av Nasjonal trusselvurdering (s. 8) at dersom hovedmålet for en offensiv nettverksoperasjon ikke er direkte oppnåelig, kan trusselaktørene iverksette nettverksoperasjoner mot leverandører og underleverandører ettersom dette kan være enklere og svært effektive veier inn mot en virksomhet eller organisasjon som er satt som hovedmål.

Norsk Senter for informasjonssikring (NorSIS) uttaler i sin trusselrapport 2019-2020 at verdikjedeangrep via leverandører utgjør en av de største truslene mot små og mellomstore virksomheter i Norge (NorSIS, 2020b) og har blitt en vanligere inngangsmetode når trusselaktøre skal angripe målrettede store virksomheter av interesse (NorSIS, 2021a). Symantec slapp sin trusselrapport i 2019 hvor de ser en økning av leverandørkjedeangrep i 2018 på hele 78% (s. 17), noe Europol bekrefter i sin rapport (2021, s. 20). I løpet av 2021 ble det avdekt og håndtert 10 alvorlige leverandørkjedeangrep i perioden juni 2020 til mai 2021, dette er ekskludert SolarWinds, et angrep som fikk stor internasjonal interesse. Det er ikke tall på antall mindre vellykkede angrep som ikke har gått noe videre, men Telenor omtaler det som betydelig mange. (Telenor, 2021, s. 42), samt at NSMs rapport om digitalt risikobilde fra 2021 viser til en tredobling av angrep i det digitale rom mot norske virksomheter, både offentlige og private i 2020 enn i 2019 (NSM, 2021a, s. 7; PST, 2022, s. 7).

Det foreligger en forventning om at leverandørkjedeangrep vil fortsette å øke ettersom flere og flere virksomheter setter vekk sine tjenester, utsetter mye av sin infrastruktur hos

tredjeparts virksomheter (Europol, 2021, s. 7), samt flere og flere enheter og mennesker vil bruke internettet for automatisering, kommunikasjon og samhandling (Telenor, 2021, s. 24). Leverandørkjedeangrep er derfor forventet å være en stor trussel og en voksende trend i årene som kommer (NorSIS, 2021b, s. 14-15).

Alle virksomheter leverer noe til noen i henhold til egen verdikjede (Telenor, 2021, s. 40) og viktigheten med å sette cybersikkerhet på kravlisten til leverandører blir her veldig gjeldende, samt at det vil være viktig å bygge gode sikkerhetsrutiner og god sikkerhetskultur på tvers av leverandørkjeder. Dette gjelder hele spekteret fra utsatt infrastruktur og tjenester til leverandører som leverer produkter og tjenester (NSM, 2022b). NSM (2020d) ser positivt på skyløsinger fremfor intern maskinvare ettersom løsningene er basert på ny og tidsriktig teknologi med mye god innebygget sikkerhet, samt at driften av skyløsningene har fokus på utvikling og oppgraderinger er lettere å gjennomføre. Dog må virksomheten ha gjort gode og riktige vurderinger i forkant av beslutningen.

I kjølvannet av krigen mellom Russland og Ukraina har cybersikkerhet vært et svært aktuelt tema hvor Nasjonalt Cybersikkerhetssenter (NCSC) i 2022 har gått ut med en oppfordring til alle norske virksomheter om å gjøre tiltak for en skjerpet digital beredskap på bakgrunn av forventede angrep (NSM, 2022c).

IKT er en del av alt dette, enten som kommunikasjons- og samhandling eller som overvåking og styring av vitale elementer, samtidig er teknologien under utvikling og kommunene ser på mulighet på kunne overvåke infrastrukturen ytterligere ved bruk av nyvinnende teknologi (StartOff, u.å). Angrep på en verdikjede som ender i kritisk infrastruktur, vil være lammende for samfunnet og derfor et aktuelt mål for større trusselaktører, som eksempelvis utenlandske statlige organisasjoner i regi av land som Kina eller Russland, som er de to aktørene som er skiltet som mest sannsynlig vil gjennomføre slike nettverksoperasjoner (PST, 2022, s. 7). Kommunene har hel- eller delansvar i mange av disse kategoriene som eksempelvis vann og avløp, helse og omsorg, kriseledelse, redningstjeneste, vei med mer, og derfor et ansvar for å sikre driften og ha kontroll på leverandørkjedene sine, foruten egen IKT-sikkerhet. Tall fra Statistisk sentralbyrå [SSB] viser at 67% av norske kommuner per 2021 har lagt en IKT-/digitaliseringsstrategi og av disse kommunene er det 82,6% som har oppdatert sine strategier. Andelen kommuner med en strategi er ikke særlig høy, men tallene viser at de kommunene som har en, også oppdaterer denne jevnlig. Statistikken sier lite om hvordan kommuner stiller seg til IKT-risiko i sine strategier, men en lagt og oppdatert strategi, vil forventes å inkludere

IKT-risiko gitt stadig økende fokus på dette fra myndighetene og andre aktører som driver med digitale trusselvurderinger.

2.2 Beredskapsprinsippene sett i lys av cyberdomenet

Selv om det brukes enorme ressurser på å utarbeide tiltak og sikre systemer mot uønskede hendelser, så har blant annet SolarWinds- og Target-sakene vist at sikkerhet i cyberdomenet kan være krevende å opprettholde. Dette har gjort at det stilles høyere krav til organisasjoner både før, under og etter hendelser.

Hovedprinsippene som legges til grunn for norsk arbeid med sikkerhet, beredskap og krisehåndtering er:

> 1. Ansvarsprinsippet: den organisasjon som har ansvar for et fagområde i en normalsituasjon, har også ansvaret for nødvendige beredskapsforberedelser og for å håndtere ekstraordinære hendelser på området.
>
> 2. Likhetsprinsippet: den organisasjon man opererer med under kriser, skal i utgangspunktet være mest mulig lik den organisasjon man har til daglig.
>
> 3. Nærhetsprinsippet: hendelser skal organisatorisk håndteres på lavest mulig nivå og beslutninger bør gjøres så tett på skadestedet som mulig.
>
> 4. Samvirkeprinsippet: myndigheter, virksomheter og etater har et selvstendig ansvar for å sikre et godt samarbeid mellom hverandre og andre med relevante, både i det forebyggende og reaktive arbeidet.

(Meld. St. 10 (2016-2017), s. 20).

Den store graden av kompleksitet, de tette koblingene og raske teknologiske utviklingen stiller kanskje for store krav til de 4 prinsippene. Cyberangrep eller -påvirkninger hvor forankringen er ukjent eller forankres internasjonalt gjør det kanskje spesielt vanskelig for ansvarsprinsippet. Disse påvirkningene kan utføres på tvers av landegrenser og tar ikke hensyn til hvem som har de forskjellige sektoransvarene eller mandat til å operere innenfor dem.

2.3 Relevant lovverk

På områder som risiko, informasjonssikkerhet, cybersikkerhet og anskaffelser i kommunal sektor er det en rekke lover som er relevante. Vi gjør derfor rede for følgende:

- Lov om kommuner og fylkeskommuner (kommuneloven)
- Lov om kommunal beredskapsplikt, sivile beskyttelses tiltak og sivilforsvaret (sivilbeskyttelsesloven)
- Lov om behandling av personopplysninger (personopplysningsloven)
- Lov om nasjonal sikkerhet (sikkerhetsloven)
- Lov om offentlige anskaffelser (anskaffelsesloven)

Formålet med lov om kommuner og fylkeskommuner er å legge til rette de nødvendige rammene for selvstyre på de lokale og regionale nivåene i Norge. Gjennom loven og etter prinsippene for lokaldemokrati skal det oppfordres til sterk deltakelse fra befolkningen. I sum skal loven bistå til å skape "effektive, tillitskapende og bærekraftige" (fylkes) kommuner. For denne oppgaven vil det være spesielt viktig å noe om lovens reguleringer angående internkontroll og interkommunalt samarbeid. Etter kapittel 25 §25-1 er kommunedirektøren ansvarlig for å sikre at lover og forskrifter følges. For å gjøre dette skal vedkommende ha et internkontrollsystem tilpasset virksomhetens størrelse, egenart, aktivitet og risikoforhold. Etter lovens sjette del, kapittel 17 – 21 har kommunene, så vel som fylkeskommuner, mulighet for å iverksette interkommunale samarbeid (Kommuneloven, 2018)

I 2010 tredde en endret lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret i kraft. Formålet med loven er bredt og skal fungere for "å beskytte liv, helse, miljø, materielle verdier og kritisk infrastruktur ved bruk av ikke-militær makt" både i krig og fredstid (Sivilbeskyttelsesloven 2010, §1). Kapittel V (5) i loven tar for seg kommunal beredskapsplikt spesifikt. Paragraf §14 sier følgende om risiko- og sårbarhetsanalyser: "Kommunen plikter å kartlegge hvilke uønskede hendelser som kan inntreffe i kommunen, vurdere sannsynligheten for at disse hendelsene inntreffer og hvordan de i så fall kan påvirke kommunen. Resultatet av dette arbeidet skal vurderes og sammenstilles i en helhetlig risiko- og sårbarhetsanalyse." Paragraf §14, tredje ledd stiller også krav til kommunene om å oppdatere analysen ved revisjon av kommunedelplaner og for øvrig ved endringer i risiko- og sårbarhetsbildet (Sivilbeskyttelsesloven, 2010).

Personopplysningsloven, i kombinasjon med personvernforordningen til EU, tredde i kraft 2018 og har til hensikt å sikre den enkeltes rettigheter om privatliv når virksomheter behandler informasjon om dem. Behandling kan blant annet være innsamling, analyse, lagring osv. Gjennom loven pålegges virksomhetene en rekke plikter og krav til etterlevelse, som i sum skal sikre den registrerte. Loven har nedslagsfelt i alle sektorer og tar ofte ikke hensyn til virksomheters størrelser. Den norske loven om personopplysninger er bygget på kravene i personvernforordningen til EU, det er derfor ikke uten grunn de er publisert sammen i den norske lovsamlingen. Det er lagt til grunn at i en konflikt mellom disse så går forordningen foran. Med det sagt, så er det stedvis i forordninger opp til det enkelte landet å bestemme hvordan personvernet skal ivaretas og på flere punkter viser også forordningen til minimumsnivå av personopplysningssikkerhet uten at den legger begrensninger på de som ønsker å være strengere/sikrere (Personopplysningsloven, 2018).

Sikkerhetsloven med tilhørende forskrifter trådte i kraft 1. januar 2019 tråde sikkerhetsloven med tilhørende forskrifter i kraft. Sikkerhetsloven er til for "å forebygge, avdekke og motvirke tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser". Nedslagsfeltet til loven er bredt og gjelder mange, blant annet statlige, fylkeskommunale og kommunale organer og leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser. Departementene har mulighet, ifølge sikkerhetsloven, å underlegge flere virksomheter under dens virke om de operer med gradert informasjon, driver aktivitet eller eier infrastruktur med relevans for grunnleggende nasjonale funksjoner (Sikkerhetsloven, 2018).

Lov om offentlige anskaffelser tredde i kraft 2017 og vi skal se spesielt nærmere på den i teorikapittelet. Veldig kort fortalt handler loven om å “fremme effektiv bruk av samfunnets ressurser”. Altså, loven er til for å regulere virksomhetene I deres anskaffelsesprosesser og skal påse at de blir gjennomført på en slik måte at de gagner samfunnet. Videre presenterer loven at grunnleggende prinsipper som “konkurranse, likebehandling, forutberegnelighet, etterprøvbarhet og forholdsmessighet” blir lagt til grunn i de offentlige anskaffelsesprosessene. Loven har flere forskrifter som aktualiserer dens virke og i sum med dem blir de kalt “anskaffelsesregelverket” (Nærings- og fiskeridepartementet, 2017).

2.4 Cyber Kill Chain for å forstå cyberangrep over nettilgang

I 2011 ga Lockheed Martin ut trusselrammeverket Cyber Kill Chain, som beskriver et cyberangrep over nettilgang med en syv-trinns lineær prosess. Virksomheter kan med kunnskap om denne prosessen plassere ut sikringstiltak for å forstyrre en trusselaktør på ulike stadium slik at de ikke oppnår sine målsetninger (Hutchins et al., 2011).

I den innledende planleggingsfasen velger inntrengeren en person eller virksomhet de ønsker å angripe. Trusselaktører utvelgelse av mål er ofte basert på kost/nytte-vurderinger, altså de balanserer innsats i form av vanskelighetsgrad, arbeidsinnsats eller risiko for fengselsstraff opp mot hvor mye de kan oppnå ved å lykkes.

Lock-heed Martin (Ibid.) tar videre for seg syv faser:

1. **Rekognosering** som innhøsting av e-postadresser, konferanseinformasjon, etc.

2. **Bevæpning** som å utnytte en bakdør i et system for å oppnå en leveringsbar nyttelast.

3. **Levering av våpen** til offeret via e-post, web, Universal Serial Bus (USB), etc. Den mest vanlige er phishing, altså levering gjennom e-post.

4. **Utnyttelse av sårbarhet** for å utføre kode på et offers system.

5. **Installasjon** av skadelig programvare på ressursen.

6. **Kommando- og kontrollkanal** for fjernmanipulering.

7. **Handlinger** på målets struktur utført med «hånd på tastatur»-tilgang eller automatiserte handlinger slik at inntrengere oppnår sine opprinnelige målsetninger

2.5 Eksempler på tidligere kjente cyberangrep

For å gi leseren en forståelse for hvem og hvordan cyberangrep kan ramme har vi valgt å ta frem noen eksempler under.

I desember 2013 ble Target (en større amerikansk dagligvare kjede) utsatt for et massivt cyberangrep hvor kundeinformasjon, inkludert kredittkortopplysninger, knyttet til 70 millioner personer ble stjålet (Jones, 2021). Basert på offentlige kilder hadde Target økonomiske skader på mer enn $200 millioner, tilsvarende 2.012.600.000 norske kroner. Angrepet er attribuert og linket til ukrainske Andrey Hodirevski også kalt Profile 958 (Weiner, 2018).

Visma hadde i 2018 et cyberangrep hvor det ble forsøkt hentet ut data. Angrepet var en nettverksoperasjon hvor metode var skadevare (Shala, 2021). Visma er en leverandør av administrative programvareløsninger og internettbaserte tjenester til små og mellomstore virksomheter i Norge, og målet var å tilegne seg tilgang på kundenettverket. De kom seg inn ved hjelp av stjålet påloggingsinformasjon, men fikk ikke tilgang til nettverket videre (NorSIS, 2020, s. 5). Dette er et klassisk leverandørkjedeangrep hvor Visma ble brukt som et ledd i en verdikjede til en større virksomhet. Denne operasjonen var en del av en koordinert handling i regi av en statlig støttet aktør i Kina (Visma, 2019).

Norsk Hydro er nok det cyberangrepet foruten Østre Toten som står sterkest i minnet når det gjelder cyberangrep mot norske virksomheter. Et cyberangrep som i 2019 startet med en uskyldig e-post fra en i organisasjonen hadde tillit til (Midtun, 2022), resulterte i en driftsstans som kostet selskapet 550-650 millioner kroner og en total ombygging av egen infrastruktur (Norsk Hydro, 2020). Dette er et stort eksempel på hvor sårbare virksomheter er og hvor viktig det er å jobbe med IKT-sikkerhet. Selv om Hydro, i motsetning til Østre Toten, fortsatt kunne bruke back-up filer og derfor hadde begrenset nedetid, tok det likevel flere uker å komme tilbake til normal drift. I et så stort selskap i et marked som er avhengig av produksjon er dette likevel kritisk.

Stortinget ble rammet av et cyberangrep i august, 2020 og våren, 2021. Det første cyberangrepet var en del av en større operasjon som hadde flere virksomheter i flere land som mål og benyttet automatisk gjetting av passord som metode. Det ble konkludert at dette var et statlig arrangert cyberangrep i regi av Russland. Det andre cyberangrepet ble gjennomført av en Kinesisk aktør hvor de fikk tilgang til Stortingets systemer via en sårbarhet i Exchange server applikasjonen (NSM, 2021a, s. 18), noe Microsoft selv ga ut en pressemelding om i mars 2021 som ble omtalt som en «Nulldagssårbarhet» med en sterk tilrådning om å gjøre mitigerende tiltak (Microsoft, 2021). En nulldagssårbarhet er en sårbarhet i et system eller en enhet som nettopp har blitt avslørt, enten på grunn trusselaktørs utnyttelse, sikkerhetstesting eller undersøkelse (Dvergsdal & Nätt, 2019). En nulldagssårbarhet utgjør høyere risiko enn andre da man i mange tilfeller ikke har kontroll over hvor de befinner seg i infrastrukturen uten nærmere undersøkelser og fordi man ikke har systemer oppdatert for å korrigere dem. Microsoft ble i eksempelet over en leverandør selv om kunden hadde kontroll på dette i egen infrastruktur, dette fordi en sårbarhet hos Microsoft blir rullet ut i infrastrukturen til kunden

Østre Toten opplevde et cyberangrep i januar 2021. Cyberangrepet har blitt definert som det verste mot en kommune i Norges historie hvor all data på en rekke systemer i kommunen ble eksfiltrert og/eller kryptert. Angriperne klarte også å nøytralisere back-up filene. I sum ble skadene så store at det tok 5 måneder å nå en tilnærmet normalsituasjon. Østre Toten sitt nivå på datasikkerhet skilte seg ikke vesentlig ut fra gjennomsnittet i norske kommuner i januar 2021 (Helgestad, 2022). De tekniske undersøkelsene utført av Atea og KPMG slo fast at det dreide seg om et løsepengevirus hvor inngangen til trusselaktøren var via enten sosial manipulasjon (phishing) hvo det ble etablert en bakdør eller via usikret fjernløsning uten to-faktor autentisering (KPMG, 2021, s. 9).

Norges Arktiske Universitet (UiT) opplevde et lignende cyberangrep som Østre Toten. Metode og måten de kom seg inn på blir beskrevet som manglende fler-faktorverifisering og sårbare systemer (NSM, 2021b, s. 13)

2.6 Leverandørkjedeangrep og typisk angrepsmetode

Når det gjelder leverandørkjede-angrep, blir det i hovedsak skilt mellom to metoder som oftest blir benyttet. Dette inkluderer både koordinerte angrep og enkeltangrep. Leverandørkjedeangrep kan skje gjennom phishing hvor det utnyttes et tillitsforhold mellom leverandør og kunde i en e-post utveksling (NSM, 2021a, s. 14). Aktøren klarer enten å komme inn på leverandørens systemer og sende e-post fra deres domener, eller klarer å forfalske adressen godt nok til at den både er troverdig og kommer gjennom filteret som er satt til å detektere uønsket e-post. I eposten vil trusselaktøren oppfordre målet til en handling, enten det er åpning av en fil som inneholder skjult skadevare klar for installasjon eller at vedkommende lures til å oppgi brukernavn/passord slik at trusselaktøren senere kan bruke tilgangen til vedkommende for videre måloppnåelse. Alt en trusselaktør trenger, er et fotfeste før de kan gå videre, enten i verdikjeden mot andre mål, eller å systematisk ta kontroll over systemer i den virksomheten som den kommuniserer med. Profesjonelle vil gjerne operere usynlig og virksomheten vil ikke merke noe til angrepet før aktøren selv gjør det synlig (Ibid, s. 17-20).

En annen metode er å snike inn sårbarheter i koder. Et eksempel her er Linux Kernel koden, som noen studenter ved et universitet i Minnesota statuerte et eksempel av. Studentene tok kontakt med Linux Kernel utviklere, introduserte seg som studenter ved universitetet, og leverte kodebidrag med bevisste «sårbarheter» som autoriserte Kernel-utviklere aksepterte og ble inkludert i den offisielle Linux-kjernen (Telenor, 2021). Denne oppgaven vil ikke

fokusere på slike former for leverandørkjedeangrep, men vi bruker dette som et eksempel på at det finnes andre måter å nå målene gjennom leveransekjeder og hvor raskt utviklingen av angrepsmåter går.

Cyberangrepet mot SolarWinds er et annet klassisk eksempel på leverandørkjedeangrep der målsettingen ikke var selskapet, men selskapets kunder (NSM, 2020a). SolarWinds leverer systemer designet for å overvåke, analysere og administrere IT-infrastruktur eksternt gjennom deres løsning kalt «Orion» (Orange Cyberdefence, 2021), hvilket betyr at de er i senter av datahåndteringen hos kunder. Ved å angripe dette systemet, fikk de tilgang til kundeporteføljens nettverk og derfra kunne de eskalere ytterligere (Marelli, 2022) ved at de plasserte skadevare i en oppdatering, en oppdatering som 18 000 kunder lastet ned (Digi, 2021). Angrepet var sporet tilbake til Russland, men Russland nekter å ha noe med angrepet å gjøre. Målene var store tunge aktører innen myndigheter, konsulentvirksomhet, teknologi, telekommunikasjon og utvinning i Nord Amerika, Europa, Asia og midt østen (Mandiant, 2022), så cyberangrepet var å anse som av internasjonal interesse. Selv om cyberangrepet ikke var direkte rettet mot Norske virksomheter, så har flere virksomheter i Norge benyttet SolarWinds sin programvare, deriblant Politiet og Statistisk sentralbyrå (Digi, 2021). Microsoft var et av målene og de hadde suksess med å etablere en bakdør som raskt ble detektert og lukket (Knudsen, 2021). NSM (2021a, s. 25) skriver i sin rapport for IKT risikobilde at dette er noe de forventer mer av i fremtiden.

Ved å bryte angrepskjede vil leverandørkjedeangrep kunne motvirkes. Dette innebærer at det må være IKT-sikkerhet gjennom segmentering av nettet, brannmurregler og kontroll på hva som er eksponert mot internett. Dette må være i alle ledd i leverandørkjeden for å kunne oppnå god nok beskyttelse (Ibid).

3 Teori

Vi har i denne oppgaven valgt å dele teorikapittelet i 3 deler. Risiko, cyber-/informasjonssikkerhet og anskaffelser. Samlet vil dette understøtte vår undersøkelse av hvordan kommuner arbeider for å håndtere risikoen for cyberangrep via leverandørers IKT tjenester. De ulike delenes rekkefølge vil gjenspeiles i både intervjuguide, analyse og drøftingsdelen av oppgaven.

Først tar vi for oss ulike fagbegreper innenfor risiko da vi ser det som overhengende for oppgaven og problemstillingen. Deretter redegjør vi for informasjonssikkerhet og cybersikkerhet, leverandørkjedeangrep og et par ulike rammeverk som kan legges til grunn i organisasjoners arbeid. Til slutt tar vi for oss anskaffelser i det brede og mer konkret mot det offentlige.

3.1 Risiko

Risiko er et bredt begrep og kan defineres som en eller en kombinasjon av flere faktorer som truer dagens eller ønsket situasjon (Renn, 2020, s. 1). Man kan også velge å se på risiko som en metode for å belyse avvik, ulykker og hendelser som truer ønsket måloppnåelse eller tilstand (Lupton, 2013, s. 3).

Risiko er mye omtalt og definert på flere måter og knyttet til usikkerhet om hendelser som gir avvik fra et planlagt eller tenkt forløp. Aven i NOU 2018:17, s. 146 beskriver risikobegrepet som:

> «... et begrep som vi bruker for å uttrykke at hendelser kan skje i fremtiden med effekter for noe som er av verdi for oss. Vi vet ikke i forkant hvilke hendelser og hvilket utfall som vil bli resultatet. Utfallet kan bli negativt eller positivt. Ofte er fokuset på uønskede og negative utfall. Effektene ses alltid ut fra en referanse, for eksempel dagens tilstand eller nivå, en normaltilstand, et planlagt nivå, eller en målsetting. Når vi snakker om risiko er som regel denne referansen underforstått, men det er viktig å klargjøre hva den er fordi ulike referanser gir ulike risikovurderinger.»

I 2015 forsøkte Society for Risk Analysis (SRA) å finne en felles måte å definere risiko på, men underveis måtte de slå seg til ro med å liste opp ulike forståelser (Vinnem & Røed, 2020, s. 25). Risiko har mange konsepter og definisjoner, men fellesnevneren for alle er at de fokuserer på forskjellen mellom muligheter og valgte handlinger, enten det er positivt eller negativt (Renn, 2008, s.1). Til syvende siste er all risiko subjektivt vurdert, dette til tross for

at det har blitt prøvd å utvikle felles definisjoner og metoder for å fremstille den objektiv. Hva som er for lav eller for høy risiko er blir opp til den enkelte å definere sannheten av (Aven, 2020, s.7). Hvor vidt mennesker har erfaring og kunnskap om risiko vil ha mye å si i risikovurderingen og -aksepten. Det er forskjellig tilnærming til risiko i de forskjellige sektorene og fagkompetanse vil gi en mer rett vurdering av risikoen (Aven, 2015, s. 13). Derfor er det viktig med tverrfaglig gruppe som er tilpasset det fagområdet hvor risikoen skal vurderes.

3.1.1 Risiko basert på trefaktormodellen

Som beskrevet ovenfor, foreligger det ulike måter å definere risiko på etter hvilket område en skal vurdere risikoen i, og i IKT sammenheng har de egne definisjoner å jobbe ut fra, eksempelvis via NS 5832:2014 hvor IKT risiko blir omtalt som et «uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet overfor den spesifiserte trusselen», også kalt trefaktormodellen (NSM, 2021b). I denne modellen tar man for seg 3 fagbegreper som alle må være til stede for å kunne definere en risiko mot et område; verdi, trussel og sårbarhet = risiko (Busmundrud, 2015, s. 32).

En sårbarhet er en svakhet (enten kjent eller ukjent) i et system, prosess eller enhet som kan bli utnyttet av en trussel til å påvirke verdiene. Innen informasjonssikkerhet er det ikke unormalt at det eksisterer sårbarheter, eksempelvis i maskinvareenheter, infrastruktur til operativsystemer, applikasjoner, moduler og drivere (NSM, 2021b). Hvert år oppdages det flere tusen programvarefeil. Disse legges ofte ut på nettsider som cve.mitre.org og nvd.nist.gov, med mindre det er en trusselaktør som oppdaget den, da blir den ofte skjult frem til dagen de bruker den aktivt mot noen.

En trussel er enhver handling (hendelse/omstendighet) som kan forstyrre, skade, ødelegge eller på annen måte påvirke en verdi negativt (og dermed en organisasjons virksomhet og drift). I et informasjonssikkerhetsperspektiv kan vi si at dette dreier seg ofte om hendelser som kan påvirke konfidensialitet, integritet og konfidensialitet.

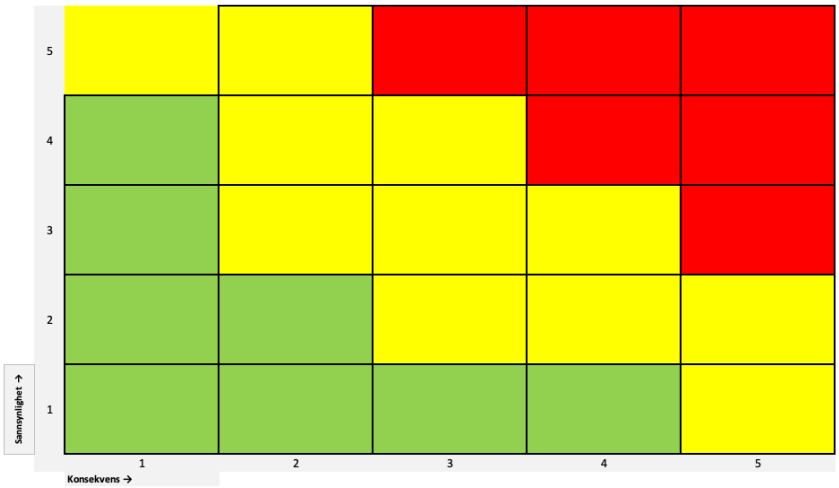
En verdi er noe en virksomhet verdsetter for å opprettholde drift, økonomi eller renomme. Dette inkluderer altså ikke bare system x, og programvare y, men også informasjon, mennesker, infrastruktur, fasiliteter, utstyr, åndsverk, teknologier og lignende. Verdiene gis forskjellige vurderinger basert på hvor viktige de er å beskytte.

Ved bruk av trekfaktormodellen kan vi nå si at risiko blir gjeldende først når en trussel har mulighet til å utnytte en sårbarhet knyttet til en verdi for virksomheten. Men med metoden skal en kunne påvirke risikoen ved enten å redusere eller forsterke beskyttelsen av verdien, fjerne sårbarheter eller eliminere trusselen. Modellen tar ikke for seg sannsynlighets beregning som de mer klassiske definisjonene (Busmundrud, 2015, s. 32-35).

3.1.2 Risiko og sårbarhetsanalyser

Et kritisk aspekt ved risikostyring er risiko- og sårbarhetsanalyser, også kalt risikovurderinger. Aktiviteten tar for seg fremstilling og sammenligning av de ulike risikoelementene på gitt fagfelt og gjengir disse som et "informativt bilde" for risikoeiere eller beslutningstakere (Aven, 2015, s. 1). For at andre skal kunne lese risikoen vil presentasjonen måtte være så detaljert som mulig slik at også andre kan vurdere risikoen på samme måte (Vinnem og Røed, 2020. s. 50)

Den mest brukte metoden å kalkulere risiko på er å se på sammenheng mellom konsekvenser og sannsynlighet. Formelen blir konsekvens x sannsynlighet = risiko i henhold til prinsippene i NS 5832:2014 og er oftest scenariobasert (Hafting, 2017, s. 364). Etter hver vurdering gir man en numerisk score, ofte 1 – 5 om hvor stor konsekvensen og sannsynlighet vil være som utgjør en maksimal risikoberegning på 25 (og kalt en 5x5 matrise). Men det vurderes også i mindre matriseskalaer som eksempelvis 2x2 (maksimal risikoberegning på 4) og 4x4 (maksimal risikoberegning på 16) (Cox, 2008). I figur 3.1 vises en risikomatrise hentet fra foreningen for Kommunal Informasjonssikkerhet (KiNS) sin mal som ligger offentlig tilgjengelig. Høye tall i risikoberegningen vil tilsi høy risiko (rød risiko) og lave tall vil tilsi lav risiko (grønn risiko).



Figur 3.1 – Risikomatrise 5x5 (Foreningen for Kommunal Informasjonssikkerhet, u.å.)

Konsekvensen av en uønsket hendelse beskriver hvor alvorlig hendelsen vil være for de verdiene du ønsker å verne. Konsekvensnivået vurderes ut fra hvilke verdier som påvirkes av hendelsen og i hvilken grad. I et informasjonssikkerhets øyemed tar man ofte spesielt hensyn til konfidensialitet, integritet og/eller tilgjengelighet.

Sannsynlighet i forbindelse med en uønsket hendelse sier noe om den forventede frekvensen man forventer at hendelsen vil oppstå. Her baserer man seg ofte på historiske data, enten fra sin egen virksomhet eller fra lignende.

Gjennom risiko og sårbarhetsanalysene benytter virksomheter ulike metoder for å identifisere risikoelementer samtidig som de vurderer sårbarhetsnivået i en infrastruktur, funksjon eller virksomheten som en helhet. Njå et al. (2020, s.285-286) har fremstilt risiko og sårbarhetsanalysers hovedfokus til å være:

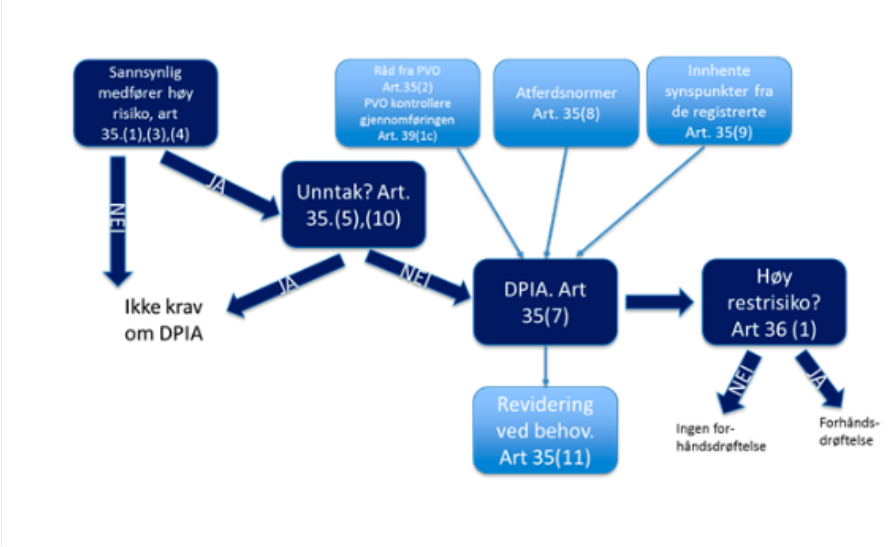
- Identifisering av hendelser - måling av eksisterende observasjoner og/eller tilgjengelig data. Er dette grunnlaget svakt, øker usikkerheten rundt hendelsen(e).
- Frekvens – måling av hvor ofte hendelser av ulik art inntreffer. Dette må sees opp mot konsekvensen av den inntrufne hendelsen for å kunne få en reell risiko.
- Årsaker - Årsaksanalyse som metode for å identifisere sammenhenger mellom ulike faktorer
- Konsekvenser – konsekvensanalyse som metode for å vurdere utfallet av tidligere inntrufne hendelser og potensielle fremtidige. Scenarioene måles ut i konsekvenser for definert verdigrunnlag fremfor annet.
- Usikkerhet – ved vurdering av sjeldnere hendelser mangler man ofte tidligere historikk som gjør risikoen lite målbar og usikkerheten blir derfor lagt til grunn i vurderingen.
- Kategoriske usikkerhetsmomenter og reduksjon av hyppighet/omfang – trefning av tiltak for å redusere sannsynlighet og konsekvens.

Som tidligere nevnt må tiltak som iverksettes og barrierene som etableres på bakgrunn av analysefremgangen over måles mot ønsket effekt slik at virksomheten har mulighet for å gjennomføre korrigeringer ved behov (Ibid, s.286).

Når man snakker om risiko, informasjonssikkerhet og cybersikkerhet sammen er det umulig å unngå å ta for seg det personvernmessige. Gjennom personvernforordningen (GDPR), som

Norge har tilsluttet seg til i lov om behandling av personopplysninger (2018), stilles det ved flere anledninger krav til virksomheter om å gjennomføre risikovurderinger. Det er spesielt i artikkel 32 og 35 det trekkes frem i forbindelse med personopplysningssikkerhet og personvernkonsekvenser. Felles mellom de ulike kapitelene går det frem at målet med vurderingene er å utvikle kunnskap om hvilke risikoer som eksisterer i behandlingen og at det skal hjelpe virksomheten i å iverksette risikoreduserende tiltak for å oppnå et akseptabelt sikkerhetsnivå. Sikkerhetsnivået skal være i stil med den typen data som forvaltes.

I figur 3.2 illustreres trinnene i en prosess for vurdering av personvernkonsekvenser.



Figur 3.2 – Prosessflyt for personvernkonsekvensvurderinger (DPIA) (Datatilsynet, 2019b)

Det er viktig å huske at gjennomføring av risikovurderinger i seg selv ikke gir økt sikkerhet og trygghet, det er først når tiltakene som er identifisert (tekniske eller organisatoriske) i disse blir utført og satt i live at nivået heves.

3.1.3 Risikostyring/-håndtering

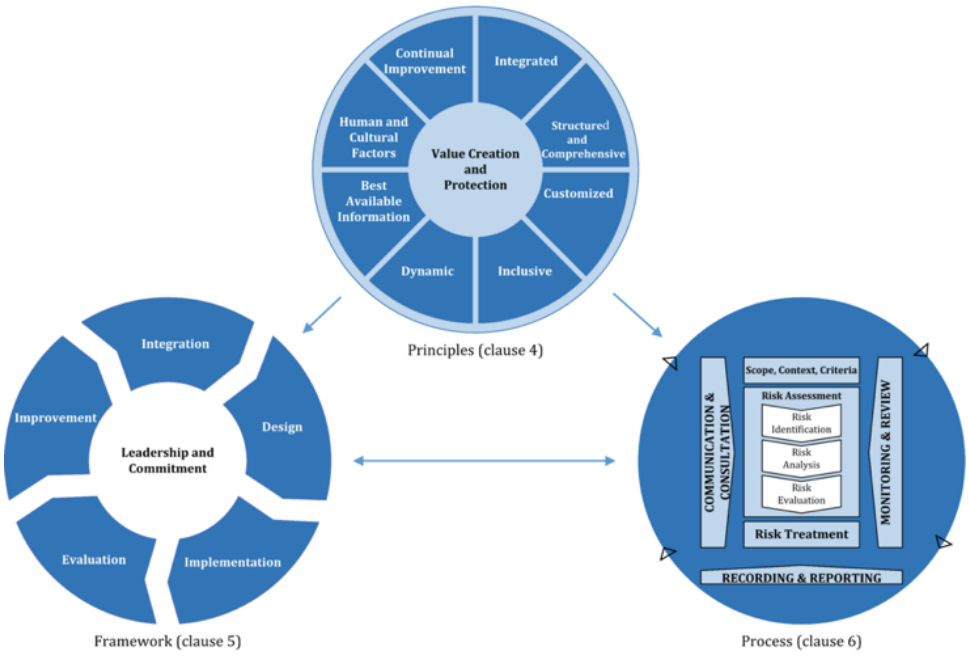
Risikostyringen går lenger ned i dybden med tanke på utforming av tiltaksplaner og implementeringen av disse. Risikoen kan endres, og kort fortalt kan vi definere risikostyring som «alle tiltak og aktiviteter som gjøres for å styre risiko (Renn, 2008, s. 1). Risikostyring handler på den ene siden om å få innsikt i risikoforhold, effekt av tiltak, grad av styrbarhet av risiko og lignende, og på den andre siden metoder, prosesser og strategier for å kunne kartlegge og styre risikoene (Aven, 2015, s. 4). Risikostyring er en kontinuerlig prosess som må gjennomføres over tid uten stopp. Når tiltak er besluttet, implementert og vurdert til ønsket effekt går man tilbake til planbordet for å vurdere risikobildet på nytt for å sikre at det ikke har utviklet seg i feil retning. Om det har skjedd, er det på nytt behov for å implementere

tiltak og fortsette overvåkingen av risikoen, og slik går sløyfen kontinuerlig (Vinnem & Røed, 2020, s. 80; Aven, 2015, s. 6).

For å lykkes med risikostyringen skriver Aven (2015, s. 5) at dette må initieres på overordnet nivå og risiko må inn i flere prosesser. Ledelsen må innføre dette i daglig drift, altså risikobasert virksomhetsstyring. Videre presiseres det 5 trinn for å få implementert risiko i virksomheten:

1. Fastsette en strategi med ambisjonsnivå (kun det mest nødvendige eller avansert risikostyring) og faste prinsipper for risikodefinisjon og -arbeid.
2. Etablere en felles risikostyringsprosess for virksomheten som alle er forpliktet å følge.
3. Organisere egen virksomhet slik at det er etableres fastsatte roller til virksomhetens risikostyring
4. Utarbeide og implementere risikosystemer, modeller, metoder og malverk med bistandsressurser
5. Kommunikasjon, opplæring og utvikling av risikokultur slik at alle får en bedre forståelse av risikoarbeidet.

For å implementere risikostyring i en virksomhet kan man ta i bruk internasjonale og utprøvde standarder. For eksempel har International Organization for Standartization (ISO) lansert ISO 31000:2018 Risk management – Guidelines som gir virksomheter et utprøvd rammeverk med en prosess for å håndtere risikoer (se figur 3.3). Rammeverket er laget på en slik at måte at det kan brukes på tvers av størrelse, aktiviteter og sektorer. ISO 31000 sikrer at man allokerer risikostyring og bruker ressurser målrettet etter en uprøvd metode (Vinnem & Røed, 2020, s. 79-80). Det er verdt å nevne at virksomheter ikke blir sertifisert etter 31000 standarden, men den gir veiledning for interne og eksterne revisjonsmuligheter.



Figur 3.3 – Kjerneelementene i ISO 31000 (ISO, 2018b).

Det vil her bli gitt en kort forklaring av den fremviste figuren. Prinsippene har til hensikt å gi veiledning i risikostyringen, hvordan verdier formidles og forklare formålene med aktivitet. Prinsippene som skisseres er grunnlaget for styringen av risikoen etter 31000. Rammeverket skal assistere organisasjon med å intrigere selve riskostring i aktivitetene og funksjonene. Prosess baserer seg på systematisk av retningslinjer, prosedyrer og praksis til bestemte aktiviteter samt kontekstureringog kontrollaktiviteter (Ibid).

3.1.4 Risikokommunikasjon og formidling

Det kan være utfordrende å formidle et klart og forståelig bilde av hva risikoen faktisk er da risikoene er dynamiske i takt med samfunnet og endringer i virksomheten. Ulikt fra den vanlige aktive kommunikasjonen i det daglige er risiko avhengig av et mangfold av kilder og gjerne over tid med tilknyttet analysearbeid. Det krever kontinuerlig vurdering av kildene som tidligere er brukt eller nye som kommer til syne, og derfor er det viktig at det innad en organisasjon jobbes etter et felles begreper og metode for risiko (Aven, 2020, s. 38).

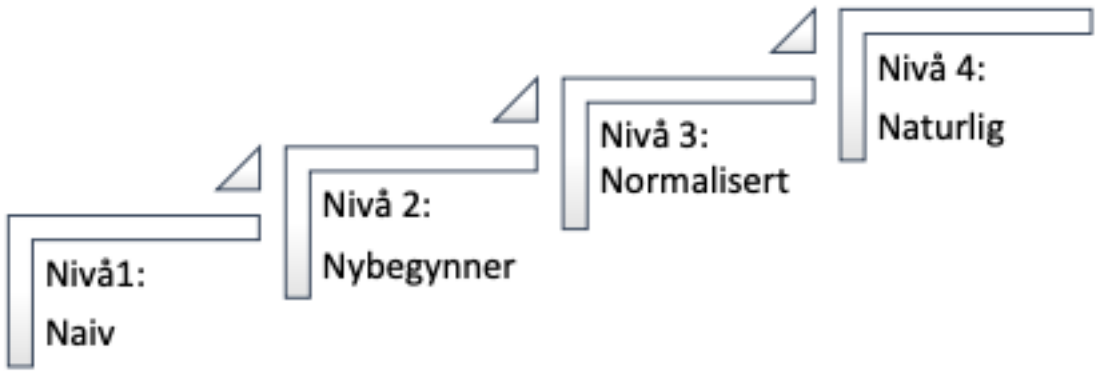
I 2010 trakk Aven og Renn frem 4 hovedformål med risikokommunikasjon:

1. Utdanning og opplysning: informere om risikobegrepet, resultater av risikoanalyser og hvordan den kan styres.
2. Risikoopplæring og insentiver til endring i atferd: informere om hvordan individer kan håndtere den potensielle risikoen som foreligger.

3. Fremme tillit til de som er utfører oppgaver innen risikoanalyse og risikostyring: styrking av syn om at arbeidet innenfor analyse og risikostyring skjer på en effektiv, tillitsskapende og akseptabel måte.
4. Involvering i risikorelaterte beslutninger og håndtering: gi de berørte interessentene og representanter fra befolkningen den informasjonen de trenger til å delta i håndteringen av risikoen.
(Aven og Renn, 2009)

Formidlingen av risiko i seg selv trenger ikke å ha som formål å forme mottakere i en bestemt retning, men skal gi individer muligheten til å bygge ytterligere forståelse for egen omverden og mulige påvirkninger som kan oppstå (Renn, 2008, s. 271). Dette vil si at det for en organisasjon vil være viktig å kunne få ansatte til å forstå hvilken risiko deres handlinger kan medføre virksomheten.

På bakgrunn av dette vil det si noe om hvilken grad av modenhet organisasjonen som helhet har for å kunne håndtere risiko, og for å kunne måle en organisasjons modenhetsgrad viser Hillsons (1997) til en 4-stegsmodell med nivåene 1-naiv, 2-nybegynner, 3-normalisert og 4-naturlig (se figur 3.4), som hjelper med å definere dette ut fra noen kriterier.



Figur 3.4 – Modell for vurdering av modenhet av organisasjonens evne til å håndtere risiko (Hillson, 1997, s. 37).

De forskjellige nivåene har en definert beskrivelse av hvordan organisasjonen som helhet jobber med risikohåndteringen, og er definert slik:

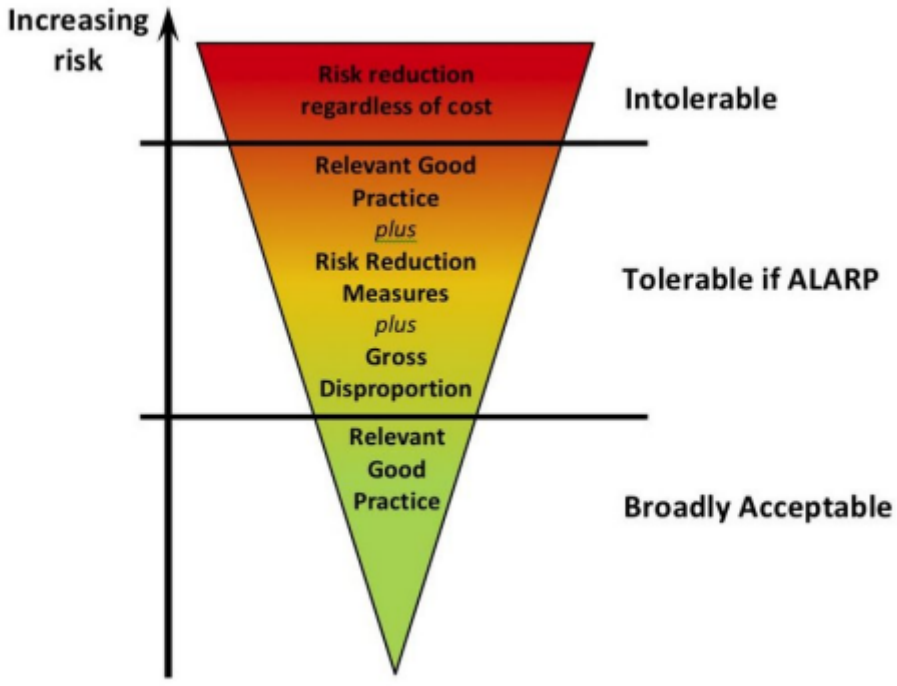
1. naiv: manglende bevissthet rundt risikostyring, gjennomføringsvegring og har ingen strukturert tilnærming til arbeidet. Det er mangelfull læring fra tidligere hendelser og klarer ikke å forutse nye trusler.

2. nybegynner: eksperimentell rundt risikohåndteringen, men mangler strukturerte prosesser og rammeverk. Arbeidet er avgrenset til noen få aktører i organisasjonen.
3. normalisert: høy grad av modenhet i sin praksis for risikohåndtering og risikostyringssystem benyttes på alle nivåer i organisasjonen, men det er ingen gjennomgående holdning til risikohåndteringen blant ansatte.
4. naturlig: gjennomgående bra styring og praksis på tvers og nedover i organisasjonen som gjenspeiles i holdninger hos ledere og ansatte gjennom oppbygd risikokultur.

Organisasjonen vurderes på kriteriene kultur, prosess, erfaring og system og på bakgrunn av dette vil de falle på et ferdighetsnivå i henhold til modellbeskrivelsen (Ibid, s. 38-39).

3.1.5 Risikoaksept - ALARP

Risikoaksept står sentralt i alt arbeid med risiko i og med at det vil alltid være noe restrisiko igjen etter implementering av tiltak. Risiko akseptkriterier hjelper oss å definere restrisikoen og handler om hvor mye av den en virksomhet kan leve med (Njå et al., 2020, s. 206).



Figur 3.5 - Risikoaksept etter ALARP-prinsippet (Cox, 2014).

Om man velger å følge ALARP prinsippet ("As Low As Reasonable Practicable" eller "så lavt som rimelig mulig"), etterstreber man å redusere restrisikoen så langt det er praktisk

mulig sett i lys av en kost- og nyttevurdering (se figur 3.5) (Vinnem & Røed, 2020, s. 537). Om en risiko ender i øverste kategori, uakseptabel, legger ALARP til grunn at det er en selvfølge at den skal ned på et lavere nivå uavhengig av kostnadsbildet tiltakene fører med seg (Aven, 2015, s. 31; Cox, 2014). Hvor grensen mellom akseptabel, tolerabel og utolerabel skal gå settes i samarbeid med en bredde av interessentene i risikostyringen, baserer seg på partenes syn på risiko og skal kunne dokumenteres (Aven, 2020, s. 6; Njå et al, 2020, s. 220-222). Kost/nytte vurderinger er et hjelpeverktøy som er en av flere metoder som benyttes når det skal tas en beslutning rundt innføring av risikoreduserende tiltak, og i denne sammenheng er det en måling av hvilken nytteeffekt tiltaket gir opp mot summen det koster å innføre det. Det foreslåtte tiltaket vil alltid måles opp mot penger og nytteeffekten må overgå summen for at det skal lønne seg å innføre det (Aven, 2020, s. 176). I vurderingen vil det være en rekke faktorer som må hensyntas og det er noen som skal vektes tyngre med tanke på hvilken verdi risikoen påvirker (eksempelvis liv/helse) eller om det eksempelvis er regulert i lovverk (Njå et al., 2020, s. 395).

3.1.6 Risiko i komplekse organisasjoner og digitale verdikjeder

Kommuner blir av Njå et al (2020, s. 130) beskrevet som et komplekst system/kompleks organisasjon. Dette begrunnes med at de er underlagt mange lover og regler, har komplekse (kontinuerlige) mål og at det er lavere risikokultur. Kommuner må jobbe med motsettende hensyn i eget virke, hvilket betyr at de i forskjellige tjenester har forskjellige forhold som de må ta hensyn til, noe som ofte går i konflikt (Jacobsen & Thorsvik, 2013, s. 40). Dette kan være lovverk, veiledninger og anbefalinger som går mot hverandre og skaper konflikt. Ifølge Charles Perrow (1999, s. 78) er komplekse organisasjoner, som kommuner, spesielt utsatt for risiko etter «normal accidents»-teorien ettersom de jobber med komplekse interaksjoner og tette koplinger. Han presiserer at enkelte systemer har risikoer som ikke kan reduseres og dermed er ulykker over tid unngåelige.

Kommuner har satte verdikjeder som er en virksomhets beskrivelse av hva som skal skape verdi (Koc & Bozdag, 2017). I motsetning til en bedrift som har fullt fokus på profitt, så er verdiene til en kommune ulikt definert (Jacobsen & Thorsvik, 2013, s. 29). Når verdikjeder blir digitale blir de komplekse, uoversiktlige, tett koplete og går på tvers av nasjoner hvor en feil i kjeden kan medføre svikt i viktige tjenesteleveranser (Lysne, 2020). Om vi legger til grunn at Normal Accidents kan gjelde for brudd på informasjonssikkerhet som en del av en kommunes digitale verdikjede kan vi argumentere med at systemer på området tross alt er

sammensatte med mange variabler. Hendelser mot disse kan dermed anses som normale, forventede og uunngåelige, men samtidig svært alvorlige. Dette betyr at målet med cybersikkerhet er å stoppe alle trusler mot virksomheten til enhver pris, men at det rett og slett er uoppnåelig i henhold til Perrow sin teori fordi hendelser til slutt vil skje i komplekse organisasjoner.

På bakgrunn av den raske utviklingen i digitale verdikjeder gjennom de to siste tiårene, fikk Direktoratet for samfunnssikkerhet og beredskap (DSB) i oppdrag om å utarbeide en risikostyringsmodell for digitale verdikjeder. Denne modellen ble utarbeidet med grunnlag i ISO 31000:2018 som vi har beskrevet over og har som mål å hjelpe utsatte virksomheter med å detektere og håndtere risikoen tidlig slik at de kan forberede seg på hendelsene som skal inntreffe (Lysne, 2020).

3.2 Cybersikkerhet og Informasjonssikkerhet

Stadig integrering av tjenesteutsatt teknologi i alle delene av norske kommuner bringer med seg flere sårbarheter og problemstillinger til en verden hvor informasjonssikkerhet og cybersikkerhet er kritisk for å opprettholde sikker tilstand og kontinuitet, både for organisasjoner og samfunnet for øvrig. Søken etter enkel tilgang og brukervennlighet har mye å si for design av teknologi og utbredelsen, men sikkerhet er ikke alltid fundamentet det blir bygget på.

Før vi går videre er det verdt å nevne at cyberangrep faller inn under kategorien for villede ondsinnede handlinger, hvor det handler om "security". Securtiy, direkte oversatt sikkerhet i denne konteksten, kan defineres som handlinger for å være beskytte verdier mot kriminalitet, vold eller annen uønsket påvirkning fra ondsinnede aktører. Sikkerhet oppnås ofte gjennom implementering av tiltak som prosedyrer, fysisk sikkerhet osv. som i sum skal avskrekke ondsinnede aktører og redusere sannsynligheten for at de lykkes i eventuelle forsøk (Engen et al, 2016, s. 26)

3.2.1 Informasjonssikkerhet

En bred definisjon av informasjonssikkerhet er aktiviteter som sikrer informasjon eller opplysninger etter prinsippene om konfidensialitet, integritet og tilgjengelighet (Datatilsynet, 2018b).

• Konfidensialitet – informasjonen skal ikke bli kjent for uvedkommende

• Integritet – informasjonen skal ikke kunne endres utilsiktet eller av uvedkommende
• Tilgjengelighet – informasjonen skal være tilgjengelig tidsriktig for autoriserte brukere ved behov (Mark et al., 2019; Datatilsynet, 2018b).

3.2.2 Cybersikkerhet

Cybersikkerhet er som tidligere nevnt et bredt begrep og brukes ofte synonymt med IKT-sikkerhet og digital sikkerhet. Vi har valgt å legge regjeringen sin definisjon til grunn. Digital sikkerhet eller cybersikkerhet tar for de aktive grep noen gjør for å beskytte og opprettholde sikker drift samt handlefrihet i cyberdomenet, enten du representerer en enkeltperson, gruppe, virksomhet eller nasjon (NOU 2015:13, 2015)

"Digital sikkerhet handler om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte avhengig av informasjons- og kommunikasjonsteknologi." (Ibid, s.32)

Cybersikkerhet er bredt begrep, og ses ofte som en forlengelse av informasjonssikkerhetsarbeidet. Man bruker å si at cybersikkerhet strekker seg fra å installere antivirus programmer på en hjemmedatamaskin, unngå svindeleposter, til forsvar av egen teknologisk infrastruktur på tvers av nivåer. Alle disse delene av cybersikkerhet kan ha relevans for enkelt personer, grupper, organisasjoner og hele nasjoner (Langø & Sandvik, 2013).

For å beskrive hvordan en virksomhet kan arbeide med informasjonssikkerhet og i forlengelse cybersikkerhet har vi valgt å legge ISO 27000 serien sentralt til grunn i denne oppgaven. Serien tar for seg både arbeid med risiko i det brede, informasjonssikkerhet, cybersikkerhet med innslag om anskaffelser og leverandøroppfølging. Vi har også valgt å ta for oss NSM sine Grunnprinsipper for IKT-sikkerhet.

3.2.3 ISO 27000-serien

ISO 27000 er en serie med standarder for informasjonssikkerhet som kan kombineres for å gi et globalt anerkjent rammeverk for informasjonssikkerhetsstyring. Serien er utarbeidet av International Organization for Standardization (ISO) og International Electrotechnical Commission (IEC), basert på dette blir navnet ofte ISO/IEC før serienummeret 27000, 27001 osv. Serien er bred i omfang og kan benyttes av organisasjoner av ulik størrelse og på tvers av sektorer. ISO/IEC utvikler kontinuerlig sine standarder i takt med teknologiens utvikling. De

ulike dokumentene i 27000 serien har blitt oppdatert ved flere anledninger, noen parallelt med hverandre og andre individuelt (ISO/IEC, 2018a)

Kort fortalt legger ISO/IEC 27000 serien opp til et overordnet styringssystem og rammeverk som er best beskrevet i 27001 med påfølgende standarder videre ut i serien som underbygger aktiviteten i systemet.

3.2.3.1 ISO/IEC 27001

I denne standarden i 27000 familien tar ISO/IEC for seg en rekke krav til etablering, implementering, vedlikehold og kontinuerlig forbedring av et ledelsessystem for informasjonssikkerhet.

27001 inneholder også forslag til krav om hvordan virksomheter kan vurdere og håndterere informasjonssikkerhetsrisikoer. Alle kravene i standeren er av en generell karakter slik at de kan bli adoptert av ulike virksomheter på tvers av bransjer og sektorer. Videre kan man også velge bort enkelte krav til fordel for andre løsninger, men ISO/IEC har spesifisert at kravene i punkt 4 til og med 10 er ufravikelige for de virksomhetene som ønsker å enten være sertifisert eller markedsføre seg med "27001 compliant" (se. figur 3.6) (Standard Norge, 2017a).

Contents Page

Figur 3.6 – Innhold i NS-EN ISO/IEC 27001:2017 (Ibid)

Under finner du en oppsummering av punktene:

Organisasjonens kontekst: Gjennom organisasjonens egen kontekst skal ledelsen definere hvilket omfang ledelsessystemet for informasjonssikkerhet skal ha.

Ledelse: Virksomhetens øverste ledelse er ansvarlig for etableringen av ledelsessystemet. Ledelsen skal sikre at nødvendig informasjon om roller, ansvar og policy er fordelt og kommunisert i egen organisasjon.

Planlegging: Virksomheten skal utføre grundige og tidsriktige vurderinger i felleskapet mellom interessenter internt, så vel som eksternt, for å utvikle et treffsikkert bilde av risikoene for så å utvikle prosess for håndtering.

Støtte: Virksomheten skal sikre at det allokeres nok og rette ressurser til arbeidet. Til slutt legger kravet om "støtte" føringer for kommunikasjon internt og eksternt.

Drift: Virksomheten skal planlegge, implementere og styre prosesser målrettet for å oppnå kravene etter standarden. Dette innebærer blant å implementere tidsriktige tiltaksplaner for å håndtere oppdukkende risikoer. Oppdatering eller utarbeidelse av nye risikovurderinger ved jevne intervaller er sentralt i arbeidet.

Prestasjonsevaluering: Virksomheten skal gjennomføre prestasjonsevalueringer ved jevne mellomrom for å vurdere etterlevelse innenfor rammen av ledelsessystemet.

Forbedring: Virksomhetene forplikter seg til å etablere prosesser for å avdekke avvik og håndtere dem gjennom tiltak.

3.2.3.2 27001: Annex A

Videre gir inneholder 27001 et vedlegg, "Annex A". Kanskje den letteste måten å beskrive dette vedlegget på er å kalle det en "katalog" over forslag til sikkerhetskontroller og mål for å håndtere indentifiserte risikoer i virksomheten.

Totalt er det 114 tiltak og sikringsmål spredt over 14 kategorier. Disse er ikke obligatoriske og trenger heller ikke følges slavisk, men skal være til hjelp under implementering av styringssystemet (ISMS). Kategoriene vi gjengir, og dens innhold er basert på 2013 versjonen. Følgende kategorier inngår i vedlegget Annex A i 2013 modellen:

A.5 Information Security Policies

A.6 Organisation of Information Security

A.7 Human Resources Security

A.8 Asset Management

A.9 Access Control

A.10 Cryptography

A.11 Physical and Environmental Security

A.12 Operational Security

A.13 Communications Security

A.14 System Acquisition, Development and Maintenance

A15 Supplier Relationships

A.16 Information Security Incident Management

A.17 Information Security Aspects of Business Continuity Management

A.18 Compliance

(Standard Norge, 2017b)

Summen av jobben som legges ned utgjør hvor god en organisasjon blir på informasjonssikkerhet, men vi anser spesielt 4 kategorier (uthevet ovenfor) i Annex A som særdeles sentrale for vår oppgave som ser på hvordan kommuner håndterer risiko gjennom leverandørers IKT gjennom gode anskaffelsesprosesser og oppfølging.

Under utdyper vi målsetningen i disse 4 og tar også for oss kontrollene. Tabellene vist i 3.2.3.2 er direkte gjengitt på sitt originale språk

A.6 Organisation of Information Security, 2 mål

Det første målet handler om å skape en organisasjon med hensiktsmessig styringsmodell og roller for å være i stand til å initiere, kontrollere og drifte informasjonssikkerhetstiltak.

Målsetning nummer to tar for seg fjernaksess. Hensikten er å ha et visst forhold til fjernarbeid og bruk av mobile enheter (Ibid, s11).

A.8 Asset Management, 3 mål

Asset management er sikringsmål som i utgangspunktet fokuserer på interne aktiviteter.

Det første målet tar for seg identifikasjon av informasjonsressurser og definisjon av passende ansvar for å beskytte dem. Dette oppnås ved å implementere en systemoversikt. (Ibid, s. 11)

Det neste målet er å sikre at informasjonen er riktig beskyttet og er en direkte forlengelse av det første. Her tar målet for seg systemoversikten og foreslår klassifisering av systemer og informasjon slik at verdiene kommer frem (Ibid, s.12)

Det siste målet i kategorien tar for seg forebygging av uautorisert tilgang, modifikasjon, fjerning eller ødeleggelse av informasjon som er lagret på infrastrukturen, altså etter kriteriene konfidensialitet, integritet og tilgjengelighet Virksomheter må etablere prosedyrene som sikrer data fra innsamling, lagring, sammenstilling og kassering (Ibid, s.12)

A.14 System Acquisition, Development and Maintenance, 2 mål.

Det første er definert som å sikre at informasjonssikkerhet er en integrert del av virksomhetens informasjonssystemer gjennom hele livssyklusen. Fra anskaffelse av nye systemer, implementering av dem og vedlikehold over tid. Her inkluderes de kravene til informasjonssystemer som eventuelt leverer skybaserte tjenester (Ibid, s.18)

Det andre målet er knyttet til det å sikre at informasjonssikkerhet er designet og implementert i informasjonssystemer i utviklingsfasen. Begge delmålene stiller krav til at virksomheten må engasjere seg i alle faser i systemers livssyklus og må i samarbeid med leverandør påse tilstrekkelig oppfølging, fra start til slutt (Ibid, s.18)

A.15 Supplier Relationships, 2 mål

Det første målet i denne kategorien er A.15.1. Målet tar for seg å beskytte infrastrukturen og/eller den informasjon som kan nås av en tredjeparts leverandører (Ibid, s.19). For å oppnå dette må virksomheten stille informasjonssikkerhetskrav, gjerne i en standard leverandørstyringspolicy, som gir føringer om hva aktører skal kunne foreta seg og hvilke tilganger de trenger for å utføre den jobben de er satt til å gjøre. Helt spesifikt hvordan dette vil se ut er ulikt fra leverandør til leverandør da man vil ha forskjellige behov ut ifra hvilken tjeneste som leveres.

Målet har 3 forslag til kontrollere som er gjengitt i rekkefølge i tabell 3.1.

A.15.1.1	Information security policy for supplier relationships	Control Information security requirements for mitigating the risks associated with supplier’s access to the organization's assets shall be

		agreed with the supplier and documented
A.15.1.2	Addressing security within supplier agreements	Control All relevant information security requirements shall be established and agree with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organizations information
A.15.1.3	Information and communication technology supply chain	Control Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain

Tabell 3.1 – tre kontrollere av leverandører ISO 27001, Annex A15 (Ibid s.19).

Det andre målet i kategorien er å opprettholde et avtalt nivå for informasjonssikkerhet og tjenestelevering, i tråd med de inngåtte avtalene (Ibid, s.19). For at en virksomhet skal kunne oppnå dette må de jevnlig gjøre avsjekk med sine leverandører, og ved enkelte tilfeller eller mellomrom også utføre tilsyn. Endring i tjenestene eller leveransen må også adresseres i denne kategorien da det vil kunne være grunnlag for oppdatering av avtalene og retningslinjene som er inngått.

Målet har 2 kontroller tilknyttet sikkerhetsmålene i A.15.2 som er gjengitt i tabell 3.2.

A.15.2.1	Monitoring and review of supplier services	Control Organizations shall regularly monitor, review and audit supplier service delivery
A.15.2.2	Managing changes to supplier services	Control Changes to the provision of service and improving existing information security policies, procedures and controls, shall be manged, taking account of the

		criticality of business information, systems and processes involved and re-assessment of risks.

Tabell 3.2 – ISO 27001, Annex A.15.2 - kontroll og endringshåndtering av leverandørtjenester (Ibid, s.19)

3.2.4 ISO/IEC 27002

27002 er i likhet med 27001 en standard i ISO 27000 serien. Dokumentet gir virksomheten forslag til ytterligere «how to» for informasjonssikkerhet, cybersikkerhet og personvern, inkludert implementeringsveiledning basert på internasjonalt anerkjent beste praksis. Dokumentet speiler 27001 Annex A, og i store trekk gir den en ytterligere veiledning og konkretisering om hvordan virksomheter kan gjennomføre grep. Tidligere i år ble 27002 revidert slik at den gjenspeiler utviklingen i samfunnet og gjeldende beste praksis på området. Det er verdt å nevne at det ikke er mulig å sertifiseres etter 27002:2022 da dokumentet kun er ment som forslag til aktiviteter for å oppnå sikringsmål. (Standard Norge, 2017c)

3.2.4 NSM grunnprinsipper for IKT-sikkerhet

Grunnprinsipper for IKT-sikkerhet fra NSM kan best beskrives som en rekke anbefalinger hvordan en virksomhet kan sikre sine informasjonssystemer. Anbefalingene til NSM kommer frem gjennom 4 kategorier hvor det underbygges med prinsipper og forslag til hvilke tiltak som kan utføre for å nå ønsket tilstand, som også vises i tabell 3.3.

De fire kategoriene er:

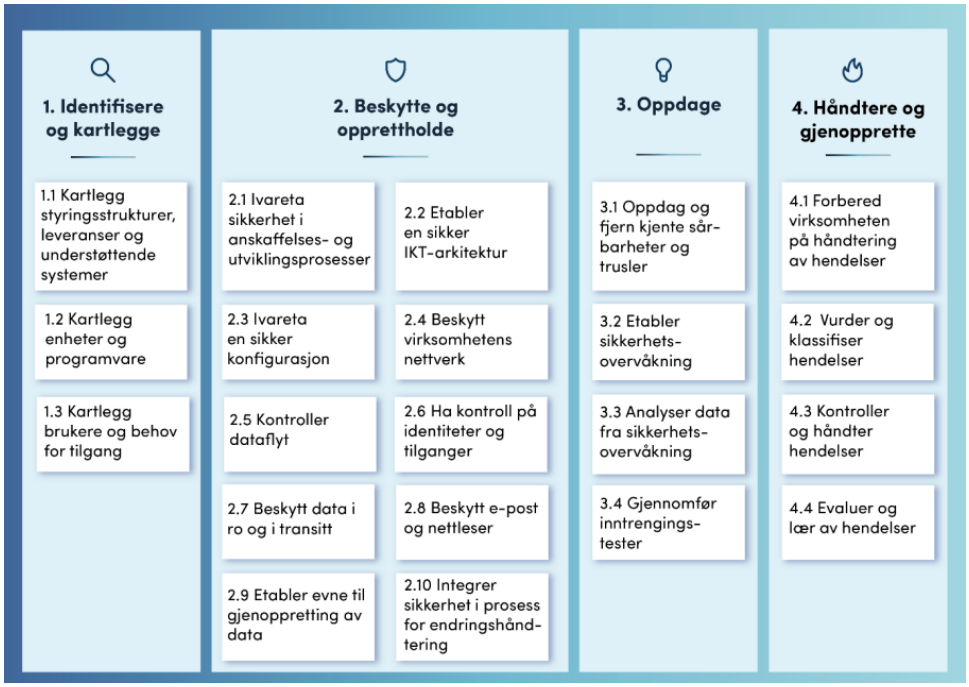
1. Kategorien «Identifisere og kartlegge» handler om det å etablere og forvalte forståelse om virksomheten herunder styringsstrukturer, ledelsesprioriteringer, leveranser, IKT-systemer og brukere.

2. Kategorien «Beskytte og opprettholde» handler om å skape og ivareta tilstrekkelig sikring av systemer samt opprettholdelses av denne. Under denne kategorien finner man prinsippene for å motstå eller begrense skaden dataangrep vil ha på virksomhetens systemer.

3. Kategorien «Oppdage» tar for seg det å oppdage og fjerne sårbarheter og trusler gjennom sårbarhetskartlegging og overvåking. Denne kan gjøres manuelt eller gjennom kontinuerlige skanninger. Kategorien tar også for seg å oppdage når systemer

går fra sikker tilstand over i en uønsket hendelse.

4. Kategorien «Håndtere og gjenopprette» tar for seg hendelseshåndtering. Dette innebærer å gjøre seg klar, håndtere hendelser, gjenopprette normaltilstand samt sikre forbedring av sikkerheten basert på erfaringer fra hendelser. (NSM, 2020b)



Tabell 3.3 - oversikt over NSM grunnprinsipper for IKT-sikkerhet (NSM, 2020e)

I likhet med ISO 27001 Annex A og 27002 er dette kun er anbefalinger uten pålegg om gjennomføring, så det er opp til hver virksomhet å vurdere hva som er relevant. I de virksomhetene som er brede og av en vis størrelse vil flere av tiltakene være relevante. NSM grunnprinsipper er ikke til for å erstatte sektorspesifikk kunnskap og regelverk, men skal være supplerende, spesielt ved kjøp av tjenester og anskaffelser.

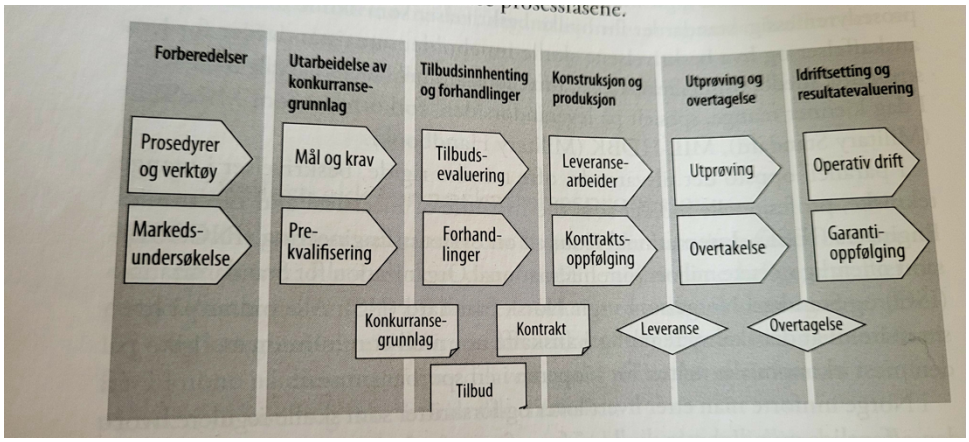
3.3 Anskaffelser

Begrepet anskaffelser er et bredt begrep og defineres ulikt mellom fagmiljøer. Vi har valgt å legge Gerhard Ihlens definisjon til grunn for denne oppgaven. Han beskriver en anskaffelsesprosess som "en prosess i bruk, mer eller mindre formell, for å foreta en anskaffelse" (Ihlen, 2014, s 20). Akkurat hva den enkelte virksomheten ønsker å anskaffe seg varierer veldig mellom virksomheter. Til tross for det brede begrepet trekker Gerhard frem en rekke likheter mellom definisjonene, blant annet at det i all hovedsak dreier seg om å anskaffe

noe for å oppnå virksomhetens overordnede målsetninger og med å gjøre det gjennom en formalisert prosess reduserer man risikoen for at man bruker tid og ressurser på noe som ikke gir effekt. Et innledende behov skal bli til løsning ved anskaffelser (Ibid, s 20).

Ihlen trekker frem 3 ulike vanskelighetsgrader for anskaffelser; enkelt, middels og stort. I det enkle tar man for seg mindre anskaffelsesobjekter uten stor grad av kompleksitet, nyvinning eller verdi. I anskaffelser hvor det anses som middels er objektet som anskaffes mer komplekst sammensatt, men hvor man gjerne utvikler kjent teknologi med middels høy verdi for virksomheten. I den siste typen av anskaffelser finner man de store og vanskelige hvor det er et komplekst og sammensatt objekt, hvor man gjerne utvikler eller tar i bruk teknologi man ikke er kjent med. For offentlig sektor er ofte anskaffelsene med stor vanskelighetsgrad også over en viss verdi som utløser krav til ekstern kvalitetssikring (Ibid, 2014, s 36).

Ihlen deler den generelle anskaffelsesprosessen inn i 6 faser med tilhørende innhold som vist i figur 3.7.



Figur 3.7 – Anskaffelsesprosessen i 6 faser (Ibid, 2014, s. 22).

Alle anskaffelser starter med en forberedelsesprosess hvor man ser på behovet man ønsker å oppnå, også kalt behovsanalyse. I denne analysen kan man for eksempel definere et IKT system til at "vi skal kunne motta denne typen data, i denne mengden, prosessere den med denne hurtigheten før den videresendes ". Analysen må ta for seg forskjellen mellom nåsituasjonen, hva kan vi gjøre med eksisterende prosesser og hvilket gap sitter vi igjen med for å oppnå ønsket evne. Det er dette gapet som skal fylles med anskaffelsen. Under denne analysen er det viktig at virksomheter bruker tiden godt og forankrer anskaffelsen på tvers av avdelinger/ansvarsområder, både for å få frem god kunnskap som ikke er synlig uten en bredde i innspill fra fagpersoner, men også slik at man erverver seg en grad av legitimitet slik at de ansatte som skal bruke løsninger ikke føler at dette er noe som blir trukket over hodene

deres uten at de har fått være med å bestemme etter medbestemmelsesretten (Ibid, 2014, s. 22).

I forbindelse med denne oppgavens avgrensning tar vi primært for oss anskaffelser for offentlig sektor.

3.3.1 Tjenesteutsetting

«Begrepet utkontraktering kan i vid forstand defineres som tjenesteutsetting eller konkurranseutsetting, og innebærer at et foretak går over til å skaffe en vare eller tjeneste fra en ekstern leverandør, i stedet for å produsere eller levere denne selv» (Kristiansen, 2015, s. 385).

Å sette ut tjenester har lenge vært en økende trend, og spesielt IKT tjenester i prosessen med å digitalisere samfunnet (NSM, 2018a). Å sette bort tjenester til en ekstern leverandør gjør at virksomheten vil kunne fokusere på sin kjernevirksomhet og fokus på økonomi er gjerne drivkraften. Det må skilles mellom private og offentlige virksomheter når det gjelder årsak til tjenesteutsetting; en privat virksomhet vil ha mer fokus på profitt og å bygge seg opp i markedet, mens offentlige virksomheter, slik som kommuner, har mer mål om å sikre rette ressurser for levere lovpålagte og utøvende tjenester til innbyggere. Anskaffelser vektes ut fra kost og kvalitet, så på sett og vis vil også kommunale anskaffelser ha fokus på pris, så sant kvaliteten er tilfredsstillende (Dimitri et al., 2011, s. 4).

Før en anskaffelse påbegynnes, gjøres en vurdering av kost/nytte. Ved utsetting av tjenester betyr at kostnaden som legges inn skal ligge under nytteverdien en får igjen (Aven et al., 2004, s. 169). Reason (1997) i Hafting (2017, s. 68) har en påstand om at lønnsom drift og sikkerhet kommer i konflikt med hverandre. Dette kan i dette tilfelle beskrives som at det på den ene siden er mål om å få mest mulig for lavest mulig kostnad, men det vil gå på akkord med kostnader knyttet til sikkerhet som er en nødvendig utgift. Her kan virksomheter ofte se seg blinde og velge å fokusere i overkant på kostnadsreduksjon. Om en kommunal virksomhet ikke erkjenner og håndterer risiko vil sannsynligheten for uønskede hendelser som truer, liv/helse, personlig sikkerhet og organisasjonens kjerneverdier øke (Weisæth og Kjeserud, 2007, s. 21).

Alle tjenester medfører en ressursbruk som må styres internt i virksomheten og ved å la en ekstern aktør levere denne tjenesten, vil administrasjonskostnadene tilknyttet leveransen være

utenfor virksomhetens daglige virke og får dermed reduserte transaksjonskostnader. Dette gjør at virksomhetene får mer tid og ressurser til å fokusere på sine kjerneverdier (Jacobsen og Thorsvik, 2013, s.224-225). Dog, må leveransen følges opp av ledelsen i virksomheten, samt det må være ressurs(er) intern i virksomheten som besitter rett kompetanse til å kunne overvåke leveransen slik at all form for administrativt arbeid vil ikke opphøre. Dersom leveransen ikke fungerer, har oppdragseier myndighet til å si opp avtalen (Kristiansen, 2015, s. 390).

Ved innkjøp av tjenester, og spesielt over tid, vil det være viktig å ivareta ressursene på lik linje som internt ansatte for å minimere risiko for dårlig kvalitet eller forsinkelse i leveransen. Jacobsen og Thorsvik (2013, s.268-269) beskriver hvordan man holder på gode ressurser gjennom satsing på ressursene gjennom eksempelvis kompetanseheving, kompensert høyere lønn eller å sette forventninger om fullførte arbeidsoppgaver med dedikerte frister for å skape relasjon mellom organisasjonen og den ansatte. Dette vil skape følelsen om gjenytelse til organisasjonen og eksempler på dette er en forståelse og spillerom virksomheten har gitt vedkommende. Disse tiltakene og forholdene vil skape et godt arbeidsmiljø og trivsel hvor virksomheten får rett person inn i rett stilling og med det lar dem videreutvikle seg. De skal alltid bety noe og lyttes til.

Ved å sette ut tjenestene vil det bety at det fremkommer en kontrakt per tjeneste, kanskje også flere underavtaler om tjenesten er stor. Dette krever ressurser for å følge opp, ikke bare ut ved første anbudsprosess, men også for å følge opp kontraktene i dens levetid før tjenesten igjen skal ut på anbud, ofte igjen med formål om lavere pris. Ressursbruken her er potensielt høy og lar man den arbeidsgruppen bli for stor, så vil formålet med utsettingen av tjenesten falle vekk ved at det påløper en økt grad av transaksjonskostnader som jo er formålet om å holde nede. Samtidig vil man i enkelte tilfeller kunne miste tilnærmingen til sitt eget virke over tid (Jacobsen og Thorsvik, 2013, s.226). Det er i slike tilfeller man må gjennomgå en grundig analysering av kost/nytte som er en lønnsomhetsanalyse der alle fordeler og ulemper belyses og som gir et resultat av lønnsomheten (Sirnes & Stoltz, 2017).

NSM (2020c) anbefaler i sin temarapport om sikkerhetsfaglige anbefalinger ved tjenesteutsetting at virksomheten ivaretar behovet for bestillerkompetanse gjennom hele livsløpet til tjenesteutsettingen, og i tabell 4.0 listes det opp en rekke kompetanseområder som de anser som viktig.

VIRKSOMHETS-KOMPETANSE	SIKKERHETS-KOMPETANSE	INTEGRASJONS-KOMPETANSE	KOMPETANSE OM ANSKAFFELSER	JURIDISK KOMPETANSE
- For å kunne definere behov og stille nødvendige krav	- For å kunne vurdere risiko og stille riktige sikkerhetskrav. Dette gjelder alle områder av sikkerhet dvs. fysisk, personell- og informasjons-sikkerhet.	- For å kunne forstå hvordan tjenestene kan integreres i virksomheten på best mulig måte	- Slik at anskaffelsen kan gjennomføres på en måte som støtter virksomhetens forretningsmessige og funksjonelle behov på best måte.	- Slik at virksomhetens juridiske krav og behov ivaretas og at kontrakten kan oppfylles i produksjonen.

Tabell 3.4 – viktige kompetanseområder ved tjenesteutsetting (NSM, 2020c).

3.3.2 Offentlige anskaffelser og regelverk

Statlige myndigheter, fylkeskommunale og kommunale myndigheter, offentligrettslige (organisert med nær tilknytning til det offentlige) og andre sammenslutninger med virksomheter som faller innunder disse er pålagt å følge lov og forskrift om offentlige anskaffelser i Norge med styring fra EØS regulativet (Nærings- og fiskeridepartementet, 2018, s. 20-21). Det er tydelige krav til utlysninger og hvilke verdier som er underlagt de forskjellige styringssettene. Lov om offentlige anskaffelser (2016, § 1) har følgende formål:

«Loven skal fremme effektiv bruk av samfunnets ressurser. Den skal også bidra til at det offentlige opptrer med integritet, slik at allmennheten har tillit til at offentlige anskaffelser skjer på en samfunnstjenlig måte»

Offentlige anskaffelser skal som hovedregel foretas etter fastsatte prosedyrer i anskaffelsesforskriften (Weltzien & Lande, 2008), og baseres på konkurranse når verdien på kontrakter for kjøp av varer, tjenester bygg/anlegg, plan/design som overstiger 100 000 kroner eksklusive merverdiavgift, hvilket betyr at anskaffelser under 100 000 kroner er unntatt anskaffelsesregelverket (Nærings- og fiskeridepartementet, 2018, s. 45), men offentlige virksomheter bør likevel etterkomme prinsippene for offentlige anskaffelser:

- *Konkurranse* – flere aktører kan på like premisser sende inn tilbud med ønske om å vinne anbudet.

- *Likebehandling* – diskriminering på grunnlag av nasjonalitet og usaklig forskjellsbehandling på annet grunnlag skal ikke skje.
- *Forutberegnelighet* – sikre forutsigbar konkurranse for leverandørene og åpenhet om alle stadier i prosessen slik at leverandørene kan ha tillitt til konkurransen og selv vurdere deltagelse.
- *Etterprøvbarhet* – leverandørene skal ha mulighet til å sjekke om oppdragsgiver har fulgt reglene for anskaffelsen.
- Forholdsmessighet – passende balanse mellom mål og virkemiddel.

(Anskaffelsesloven, 2016, §4; Nærings- og fiskeridepartementet, 2018, s. 59-60).

Som EØS land, så er det en rekke terskelverdier en offentlig virksomhet må forholde seg til når summen overstiger 100 000 kroner, og det skilles mellom nasjonale og EØS nivåer. I tabell 3.5 og 3.6 gjør vi rede for de terskelverdiene på nasjonalt nivå og EØS nivå som kommunene må forholde seg til.

Nasjonale terskelverdier for kommuner

Terskelverdi	Type anskaffelse	Henvisning til anskaffelsesforskriften
100.000	Alle anskaffelser som er omfattet av forskriften	§ 1-1 (og anskaffelsesloven § 2)
1,3 millioner	Anskaffelser av varer, tjenester og bygge- og anleggsarbeid	§ 5-1 (2) bokstav a
1,3 millioner	Særlige tjenester	§ 5-1 (2) bokstav b

Tabell 3.5 – nasjonale terskelverdier for kommuner (Nærings- og fiskeridepartementet, 2018, s. 47-48; Vigander, 2022).

EØS-terskelverdier for kommuner

Terskelverdi	Type anskaffelse	Henvisning til anskaffelsesforskriften
2,2 millioner	Vare- tjenestekontrakter for kommuner, fylkeskommuner og offentligrettslige organers vare- og tjenestekontrakter	§ 5-3 (1) bokstav b
56 millioner	Bygge- og anleggskontrakter for kommuner, fylkeskommuner og offentligrettslige organers vare- og tjenestekontrakter	§ 5-3 (1) bokstav c
10 millioner	Kontrakter om helse- og sosialtjenester Kontrakter om særlige tjenester	§ 5-3 (2)

Tabell 3.6 – EØS terskelverdier for kommuner (Nærings- og fiskeridepartementet, 2018, s. 47-48; Vigander, 2022).

Når en kommune skal gjøre en anskaffelse, så vil det være bestemte krav ut fra hvilken terskelverdi anskaffelsen har. Mens det i mindre anskaffelser ikke stilles krav til kontroll på leverandørkjeden gjennom å konkretisere antall ledd og krav til funksjonene mellom leddene, vil det i større konkurranser som overstiger den nasjonalt satte terskelverdien på over 1,3 millioner være krav til dette (Markussen, 2017).

Ifølge Direktoratet for forvaltning og økonomistyring (DFØ) består offentlige anskaffelser av tre hoveddeler hvor hver del har flere prosesser. Disse prossene ligner mye på modellen til Ihlen som beskrevet lengre opp (se figur 3.7), men mens Ihlen har en generell anskaffelsesprosess, vil denne modellen vise hvordan den vil være i en offentlig anskaffelse. I figur 3.8 vises de tre hoveddelene med underliggende prosesser oppnevnt under hver del.

Avklare behov og forberede konkurransen	Kontrakts -gjennomføring	Kontrakts -oppfølging
- Invitasjon til konkurranse - Følge opp konkurransen/ svare ut innkommende spørsmål - Justere/endre ved behov. - Evaluere og vurdere tilbydere og tilbud. - Tildeling kontrakt - Kunngjøring av valg - Evaluere konkurransen -	- Behovsvurdering - Etablere kontraktsstrategi - Forberede konkurransen - Lage konkurransegrunnlag - Definere spesifikasjoner, krav, kriterier og kontraktsvilkår - Definere kvalifikasjonskrav	- Sikre rutiner, frister, ansvar, fremdrift og krav til kvalitet blir fulgt opp - Følge avtalens bestemmelser for oppgjør, bestillinger og evt. Itenciver. - Oppfølging kunde/leverandør - Håndtere endringer - Avslutte kontrakt - Sluttevaluering

Figur 3.8 - tre hoveddeler i en offentlig anskaffelse med underliggende oppgaver/prosesser (Anskaffelser, 2022).

I offentlige anskaffelser er det størst påvirkningskraft i første del til å komme med krav til leverandørers IKT tjenester, hvor det senere ut i prosessene både ha en konsekvens for kvalitet, konkurransens prosess og pris (Methi, 2016).

Om en kommune avviker fra de anbudsrettslige prinsippene og regelverket om offentlige anskaffelser, vil den som oppdragsgiver stå ovenfor en risiko for å bli møtt med et krav om erstatning fra anbydere som mener seg ulovlig forbigått, samt et overtredelsesgebyr med et tak på 15% av anskaffelsens verdi (Anskaffelsesloven, 2016, §10 & §12). Størrelse på

erstatningen til anbyder avhenger av hvor vidt oppdragsgiver må betale på bakgrunn av positiv kontraktsinteresse (estimert tap som anbyder kan dokumentere de går glipp av ved uteblivelse) eller negativ kontraktsinteresse (beregnet tap som anbyder har påløpt ved å utarbeide anbudet). Det er mest vanlig at anbydere kun får kreve erstatning etter negativ kontraktsinteresse (Seim, 2002).

I enkelte tilfeller, basert på tidspress før oppdragets start, tillates det at oppdragsgiver i stedet går i direkte dialog og forhandling med én eller flere leverandører. Slike hasteanskaffelser er under gitte forutsetninger tillatt både over og under EØS-terskelverdien. Kriteriene for dette er strenge, og desto høyere terskelverdien er, desto strengere krav (Weltzien & Lande, 2008).

Det er med formål om å minimere usikkerheten ved å inngå en kontrakt da partene må sette seg ned og konkretisere produktet/tjenesten, dette blir også omtalt som en *bytteavtale* ettersom det inngås en avtale om en tjeneste eller et produkt mot økonomiske midler (kan også være tjeneste/produkt mot tjeneste/produkt, men anses å være mindre vanlig). Slike anskaffelser er ofte komplekse og det må settes av tid til å spesifisere leveransen, velge rett leverandør, samt valg av kontraktsform (Karlsen, 2018, s. 196-197). Kontrakten bør og inneholde punkter rundt leveransekvalitet, rapportering, endringsprosesser, revisjon, terminering og møtearenaer (NSM, 2018-a)

Når anskaffelsen har kommet så langt at det står mellom flere tilbud, så må utlysende aktør sette opp en rekke prosesser for å sikre god kontrakts strategi og Karlsen (2018m s. 198) foreslår en prosesslinje som vil være aktuell ved større anbud uavhengig privat eller offentlig sektor:

Det finnes flere føringer i form av lovverk som anskaffelsesloven (2016, §2) og anskaffelsesforskriften (2016, §1-2) som kommuner må forholde seg til. Og for å avhjelpe med et komplekst lovverk, så finnes det veiledere som eksempelvis veiledning til anskaffelsesforskriften som er et insentiv fra Nærings- og fiskeridepartementet (2018, s. 17) med formål om å få et krevende og omfattende regelverk til å bli mer forståelig.

Likevel er det tung materie og det finnes derfor virksomheter som skal bistå blant annet kommuner i en slik prosess. Direktoratet for forvaltning og økonomistyring (DFØ) har etablert en egen divisjon for offentlige anskaffelser som leverer produkter og tjenester som malverk, veiledning og rådgivning (DFØ, 2021a). Innen malverk har DFØ lagt ut statens standardavtaler (SSA) med egne utforminger for kjøp av IT-produkter, skyløsninger, programvare med databehandleravtale og sjekkliste som går på personvernlovgivningen.

Innen mal for oppdragsavtale (SSA-O) eller i kjøpsavtalen for kjøp av IT-utstyr (SSA-K) er det i den generelle avtaleteksten ikke spesielt definerte krav til leverandørkjeden annet enn at de skal:

«...påse at leverandør(er) av tredjepartsleveranser foretar tilstrekkelig og nødvendig sikring av Kundens data» (DFØ, 2019a, s.10)

og

«*Leverandøren skal iverksette forholdsmessige tiltak for å ivareta krav til informasjonssikkerhet i forbindelse med gjennomføring av tjenesten»* (DFØ, 2019b, s. 28).

3.3.3 Risiko ved kjøp via eksterne leverandører

«Vi i NSM er bekymret for at vurdering av sikkerhetsrisiko og etablering av sikringstiltak ikke får prioritet ved tjenesteutsetting.» (NSM, 2018b)

Å eliminere intern risiko som er tilknyttet en intern oppgave, er ifølge Jacobsen og Thorsvik (2013, s. 224-225) hovedformålet til en virksomhet ved å sette den vekk, samtidig som det er ønskelig å få samme oppgaven til en lavere pris. For kommuners del, er det et satt regelverk for hvordan anskaffelser skal gjennomføres og hvilke terskelverdier som gjelder (se over), men til tross de mange fordelene denne type aktivitet kan bidra til, innebærer det også utfordringer og risikoer som kan lede til uønskede konsekvenser (Fan et al., 2012). Foruten at det blir en forlengelse og avhengighet innen leverandørkjeden, der enhver feil kan føre til forstyrrelser i leverandørnettverket (Lee et al., 2012), er det en generell usikkerhet og bekymring når det gjelder sikkerhet og etterlevelse av eksterne og interne krav (Bachlechner, Thalmann & Maier, 2013), spesielt når det gjelder konfidensialitet og uautorisert tilgang til private og sensitive data, som kan kompromittere en virksomhet (Frost, 2000; Prado, 2011).

Mye kan løses ved at de inkluderer krav til leverandørenes IKT-sikkerhet. Men ved å redusere annen risiko ved å sette vekk tjenesten uten å stille riktige krav, så vil det være en udefinert risiko for leverandørkjedeangrep, mulig stor risiko dersom leverandøren har dårlig IKT-sikkerhet. Offentlige og private virksomheter ser på IKT og bruken av IKT som en viktig del av virksomheten og realisering av sin strategi, men NSM viser til bekymring rundt at det kun vurderes risiko knyttet til økonomi og gjennomføringsevne og at videre vurdering av risiko ikke gjennomføres (2018a).

Når en kommunes leverandør benytter en underleverandør som skal følge de samme kravene som står i utlysningen, blir det enda viktigere å sikre riktige krav til IKT-sikkerhet innad i leverandørkjeden. Her ser vi at malverket og veiledningene sier lite om hvilke krav til IKT-sikkerhet kommunene må stille til tilbyder(e), annet enn at det må beskrives i kravspesifikasjonen, også referert til som bilag 1 ved utlysning (DFØ, 2020, s. 13; DFØ, 2019b, s. 28) og krav til leverandørkjedens IKT sikkerhetsoppbygging kan i mange tilfeller glippe.

En av fordelene med å sette vekk tjenester er at leverandører besitter rett kompetanse og kan gjøre justeringer på en bedre måte, men det åpner samtidig en risiko dersom det ikke også i kommunen sitter ressurser med rett kompetanse som kan stille krav til leverandørene, IKT-sikkerhet og leveranse, samt overholde kontroll på virksomhetens risiko mot leveransen.

Eksempler på risikoelementer som er aktuelle ved en tjenesteutsetting er:

- redusert kontroll på stadig mer komplekse verdikjeder
- tap av intern kompetanse
- avhengigheter til eksterne tjenesteleverandører for å kunne levere virksomhetens tjenester.

Det foreligger også en anbefaling om at selve leverandøren får krav og følges opp vedrørende leveranseevne og muligheten til å vedlikeholde ønsket sikkerhetstilstand (NSM, 2018b).

En leverandør og kunde vil alltid inneha en form for risiko på hver sin side, Den beste løsningen er om den kartlegges sammen og det finnes tiltak for å motvirke risikoen, sammen. Dette er ikke er enkel prosess ettersom ingen av partene ønsker å påta seg mer risiko enn nødvendig. Det er en klar fordel om risikoen kan fordeles mellom kunde og leverandør. Mye av risikoen kan reduseres for kjøper gjennom god dokumentasjon, gode kravstillinger, opparbeidet relasjon og tillit, samt tydelig satte mål og delmål (ibid).

3.3.4 Valg av leverandør(er)

Kriterier for evaluering av innkommende tilbud/anbud før valg av leverandør. Kriteriene må speile det behovet som virksomheten setter, gjerne pris først og fremst, men også andre kriterier som kvalitet, tekniske forhold, gjennomføringsevne, kommersielle forhold og risiko (Ihlen, 2014, 2014, s.142).

Ved store kontrakter og mange innkommende tilbud vil det være en fordel for kunde å pre-kvalifisere leverandører for å få en kortere liste med tilbud som skal evalueres nærmere

ettersom dette er svært ressurskrevende for både kunde og leverandører. Pre-kvalifiseringen vil da stille mer spesifikke krav til leverandørene som eksempelvis skadestatistikk, teknisk kapasitet/ekspertise, prosjektkompetanse, tilgjengelig kapasitet, ressurser, kompetanse og personell, tidligere prosjektoppdrag som ligner kundens, leverandøren økonomiske styrke og prisnivå på tidligere leverte anbud (Ihlen, 2014, s.140)

Når kunden sitter med en anselig mengde tilbud/anbud vil selve evalueringen finne sted og det er noen forhold som stiller seg sterkt som vektingskriteriene kost og kvalitet. Men det er ikke dermed sagt at dersom en leverandør scorer høyt på et vektingskriterium, så vil de likevel ikke vinne dersom de scorer lavt på det andre kriteriet (Ihlen, 2014, s. 154). Eksempelvis om kost er vektet 60% og kvalitet er vektet 40% av en total score på 100%, så vil en leverandør måtte score nokså høyt også på kvalitet dersom de ønsker å vinne anbudet. Hva som setter kriteriene for kvalitet kan være litt forskjellig, men det er viktig at forholdene kan vurderes konkret mellom leverandørene slik at det blir en rettferdig prosess. En viss grad av åpenhet er også lurt å ha mot leverandørene når evalueringen er ferdigstilt, men i offentlige virksomheter er det ofte at noen opplysninger unndras offentligheten av hensyn til bestemmelser i offentlighetsloven, eller anbud som er underlagt sikkerhetsloven.

Etter man har valgt en leverandør går man over i et *forhandlingsstadium* hvor man med en eller flere leverandører ser på hvordan løsningene kan justere for å treffe virksomheten enda bedre, samt hvordan dette vil slå ut på pris og risiko (Ibid). Noen leverandører er såpass svære og med et svært system at de blir sett på som mektigere enn kundene deres (en liten kommune vs Microsoft). Det kan virke håpløst å forhandle om strenge retningslinjer og krav som du vet tidlig at leverandørene ikke vil følge. I enkelte tilfeller må du kanskje velge å stole på deres standardpolicyer, kontroller og kontrakter fordi du trenger tjenesten sårt.

Når man har falt på hvilken leverandør man ønsker ser man på kontraktsformen og/eller relasjonsform. Dette er ulikt i forhold til hvor stor kontrakten er i verdi og omfang. Mindre og korte oppdrag kan med fordel inngås med forenklede kontrakter, mens oppdrag med større verdier, større omfang og over lengre tid krever mer komplekse kontrakter (Karlsen 2018, s. 208). Å forvalte en kontrakt over tid fra begge parter vil i tilfeller være krevende. Som vi tidligere har vært inne på, så er det å ha intern kompetanse om leveransen på kundens side en klar fordel for å kunne håndtere kontrakten, endringer og konflikter. Leverandøren har ofte denne kompetansen, men dersom kunden mangler dette vil det være ødeleggende for både

relasjon, tillitt og leveranse. Foruten intern kompetanse er det noen rutiner som kan lette arbeidet med å håndtere kontrakten:

- Gjennomgang av kontrakten og leverandørens arbeid. Dette i form av faste møter med leverandøren hvor fremdrift, utfordringer og avklaringer vil være aktuelle temaer.
- Gode rutiner for betaling av fakturaer til leverandøren gjennom avtaleperioden
- Raske beslutninger og avklaringsprosesser ved behov for endringer
- Håndtere konfliktene med en gang de dukker opp og finne løsninger for begge parter (Ibid, s. 214)

4 Metode

Formålet vårt har vært å forstå hvordan norske kommuner jobber med leverandører for å håndtere risiko for leverandørkjedeangrep, hvordan de vurderer myndighetenes arbeid med risiko og cybersikkerhet og hvordan kommunene innfører cybersikkerhet i deres anskaffelsesprosesser. Dataene er innsamlet ved hjelp av et metodisk rammeverk som beskrives i denne delen.

4.1 Forskningsmetode

Ettersom vi i problemstillingen benytter spørsmålsformen «hvordan» og med det ønsker å studere enkelthendelser, gå i dybden på problemstillingen, belyse små detaljer og gi nøye utvalgte informanter fra spesifikke virksomheter større frihet til å uttrykke seg med mål om å få relevant kunnskap om temaet i et spisset og avgrenset forskningsområde, er kvalitativ forskningsmetode med intervjuer valgt som forskningsmetode (Johannesen et al., 2016, s. 145; Thurén, 2015, s. 123).

Vi ønsker å se på problemstillingen fra 3 vinkler: tre aktuelle kommuner med 25 000 – 35 000 innbyggere, fageksperter fra privat og offentlig sektor med virke inn mot kommunenes arbeid og en interkommunal samarbeidsvirksomhet (IKS) som jobber opp mot flere kommuner. De sistnevnte vinklingene vil være understøttende for problemstillingen og oppgavens tyngdepunkt som omhandler kommunene og deres arbeid. I figur 4.1 illustrerer vi hvordan vi tenker.

Figur 4.1 – aktørvinklinger og sammenligning mot problemstilling.

En annen vinkling på denne oppgaven er å kartlegge videre arbeid og utvikle nye perspektiver og problemstillinger for fremtidig forskning. Da fokuset på valgte tema er forholdsvis lite i den store sammenheng, så vil vi legge et grunnlag for videre forskning som gjør at dette kan belyses fra flere ulike kanter. Det vil derfor være relevant å tilnærme seg gjennom eksplorative undersøkelser som et delmål (Johannesen et al., 2016, s. 53).

4.2 Forskningsdesign

Ettersom det var en spesifikk tilnærming med et mål om å gå i dybden av problemstillingen, måtte vi ha en dyptgående forståelse av hvordan kommunene jobbet med risiko, cyber-/informasjonssikkerhet og anskaffelser. Grunnet sentrale kjennetegn som avgrenset interesseområde med behov for mest mulig detaljert beskrivelse, et eksplorativt formål, samt behov for datainnsamling gjennom et avgrenset antall enheter i et tidsavgrenset perspektiv, så falt valget på casedesign som forskningsstrategi (Ibid, s. 80-81).

I henhold til vår problemstilling ønsket vi å se på tre kommuners risikohåndtering av leverandørkjedeangrep. Dette var et avgrenset og spisset område (tre ulike case), og samtidig valgte vi å hente data fra tre ulike roller i de tre kommunene (enheter) og sammenlignet resultatene fra disse. Vi valgte og å hente inn faglige ekspertvurderinger av samme problemstilling. I tillegg så vi på kommunenes opplevelse av myndighetenes arbeid med risiko, cybersikkerhet og informasjonssikkerhet mot kommunene, samt hvordan kommunene implementerte cybersikkerhet og informasjonssikkerhet i anskaffelsene (Ibid, s. 206). Ettersom casestudier ofte benyttes i organisasjons- og samfunnsforskning og metoden egner seg til å finne svar på hvordan noe skjer, så vurderte vi at dette forskningsdesinget traff problemstillingen vår godt. Intervjuobjektene var avgrenset og strategisk plukket ut for å få mest mulig informasjon ut av færrest mulig intervjuer. I arbeidet med datainnhentingen, koblet vi stoffet mot den generelle forståelsen vi hadde, samt fikk en dypere forståelse av stoffet (Ibid, s. 208-212).

4.3 Intervju

I denne oppgaven benyttet vi kvalitative dybdeintervjuer i et semistrukturert oppsett med beskrivende spørsmålsform med en spesifikk retning som datainnsamlingsmetode, ettersom vi hadde en forventning om at intervjuene ville måtte justeres underveis (Ibid, s. 148). Vi ønsket å intervjue informanter som har temaet som en del av sin rollebeskrivelse og som jobber med

dette til daglig. På denne måten fikk vi en bred forståelse av temaet og derav en tydeliggjøring av problemstillingen vår.

Alle intervjuene ble tatt opp audiovisuelt for å lettere kunne transkribere og hente ut all relevant data i etterkant. Beslutningen falt på dette for å kunne fokusere på den gode samtalen og for å vie mer fokus på å bygge relasjon med informantene (Ibid, s. 146).

Fremgangsmetoden var i form av en utarbeidet intervjuguide som ble ført av oss hvor én stilte spørsmål og førte samtalen, mens den andre tok notater i stikkordsform for å forenkle prosessen og håndterte det tekniske.

4.3.1 Informanter

Vi var veldig selektive når det gjaldt valg av informanter vi ønsket et intervju med grunnet tidsperspektiv og mengde analysearbeid som ville tilkomme i ettertid. Og på samme grunnlag ble det vurdert og besluttet å sette et tak for antall intervjuobjekter (Ibid, s. 95-96). Formålet var å hente mye informasjon ut fra et så snevert område som mulig, det vil si at i denne sammenheng ikke var relevant med for mange informanter, men heller avgrense til noen strategiske aktører (Ibid, s. 113).

Basert på tidligere skisserte vinklinger for vår oppgave var vår utvalgsstrategi (utvalg av målgruppe og informanter innenfor denne/disse målgruppene) å velge ut informanter innenfor de nevnte målgruppene. Antall informanter var i forhold til tilgjengelighet, men målet var et sted mellom 10 og 15 stykker. Vår strategi ble som vist i tabell 4.1.

Kommune 1 (Case 1)	**Kommune 2** (Case 2)	**Kommune 3** (Case 3)	**Fagintervju privat sektor**	**Fagintervju offentlig sektor**	**IKS virksomhet**
Ansvarlig innen anskaffelser	Ansvarlig innen anskaffelser	Ansvarlig innen anskaffelser	Person med kompetanse innen kommunalt arbeid	Ansvarlig risiko	Ansvarlig innen risiko
Ansvarlig informasjonssikkerhet	Ansvarlig informasjonssikkerhet	Ansvarlig informasjonssikkerhet			Ansvarlig informasjonssikkerhet
Ansvar innen risiko	Ansvar innen risiko	Ansvar innen risiko			

Tabell 4.1 – strategi for utvelgelse av informanter.

Det var viktig for oss og oppgavens oppbygging at vi håndplukket kommunale virksomheter som var av lik størrelsesorden da dette hadde, etter vår mening, best forutsetninger for å gode

kvalitative data og sammenligningsgrunnlag gitt lik organisering og ansvar. Vi landet derfor på kommuner med 25 000 – 35 000 innbyggere spredt utover Norge.

Det ble benyttet direkte avtale med de respektive per e-post eller telefon for å avtale intervju etter en fremstilling av problemstilling og forskningsspørsmålets formål (Ibid, s. 113-126). Alle aktørene som ble forespurt om intervju fikk informasjon om oppgaven, våre beslutninger rundt gjennomførelse, personvern og tidsbruk, samt tilsendt en samtykkeerklæring (se vedlegg 1).

Det ble sendt ut en bred forespørsel til de kommunene innenfor den størrelsesorden. Årsaken til at vi gikk bredt ut, var fordi vi forventet manglende svar fra de fleste, noe vi fikk rett i og vi brukte mye tid på oppfølging via telefon for å lande nok kandidater. Vi var mer målrettet når vi skulle finne aktører til fagintervjuene og IKS virksomheten, og de informantene vi forespurte var utelukkende positive til det og vi fant snarlig en dato/tid som passet. Totalt sett endte vi opp med 14 informanter, som var i det øvre sjiktet av det antallet vi så for oss og fordelingen vises i tabell 4.2 som bygger på tabell 4.1.

Kommune 1 (Case 1)	**Kommune 2** (Case 2)	**Kommune 3** (Case 3)	**Orange Cyberdefence**	**Kommune-CSIRT**	**IKS virksomhet**
Anskaffelser – informant 6	Anskaffelser – informant 13	Anskaffelser – informant 12	Person med kompetanse innen kommunalt arbeid – informant 1	Person med kompetanse innen kommunalt arbeid – informant 7	Risiko og informasjonssikkerhet – informant 2
Informasjonssikkerhet – informant 4	Informasjonssikkerhet – informant 9	Informasjonssikkerhet – informant 14		Teknisk kunnskap – informant 8	Anskaffelser – informant 3
Risiko – informant 5	Risiko – informant 10	Risiko – informant 11			

Tabell 4.2 – oversikt over informanter per virksomhet.

Med formål om å oppnå et oppriktig og fyldig syn på temaet og problemstillingen, ønsket vi å gjennomføre intervjuene på informantenes egen arena og gjerne et fysisk ansikt-til-ansikt intervju der det var mulig, men i flere tilfeller måtte vi benytte Microsoft Teams grunnet lang avstand mellom oss og informantene, samt stedvis tidspress.

4.3.2 Intervjuguide

Det ble utarbeidet intervjuguider som var tilpasset til de ulike aktørene basert på våre teoretiske antagelser slik at vi fikk frem ønsket data. Intervjuguiden tilpasset kommunene og IKS-virksomheten hadde en tyngde mot risiko, cybersikkerhet/informasjonssikkerhet og anskaffelser, samt at de tok for seg spørsmål om deres opplevelse av myndighetenes arbeid med risiko, cybersikkerhet og informasjonssikkerhet (se vedlegg 2). Intervjuguidene vi benyttet til intervjuene med fagekspertene var tilpasset deres virke mot kommunene og deres

syn på kommunenes arbeid, samt at de også fikk spørsmål om myndighetenes arbeid med risiko og cybersikkerhet/informasjonssikkerhet.

Ved å legge opp intervjuene som semistrukturerte med beskrivende spørsmålsform fikk vi anledning til å justere etter hvert som vi gikk gjennom listen der vi så at det kom tilfeller hvor spørsmålene ville sammenfalle eller at noen nye dukket opp (Johannesen et al., 2016, s. 148).

4.3.3 Gjennomføring av intervjuene

Foruten god datainnsamling, var formålet med intervjuene å oppnå en god relasjon, samt en felles forståelse av temaet og problemstillingen. Primært var det to-til-en intervjuer hvor vi var to fra UiS og én fra virksomheten. Ved ett tilfelle gjennomførte vi også et to-til-to intervju da dette var praktisk best for virksomheten.

Samtalene startet med en presentasjon av forskerne, og det ble gitt informasjon om innsamlingsmetode, lagringstid/-måte, presentasjon av temaet og informasjon om ivaretakelse av deres anonymitet med nok en påminnelse om samtykke og mulighetene for å trekke dette. Samlet sett og med en forberedt intervjuguide følte vi at vi hadde et godt grunnlag for innhenting av data og at forholdet mellom informant og forskere var bra.

Intervjuene var satt til å vare i 45-60 minutter hvor vi i enkelte tilfeller gikk over, mens vi i andre tilfeller kunne avslutte før. Inntrykket var at spørsmålene var riktig formulert og det var kun ved et tilfelle at det kom et tilleggsspørsmål fra informantens ståsted. Etter hvert intervju ble notatene gjennomgått og raskt evaluert i tilfelle det skulle være behov for ytterligere avklaringer som da i tilfelle ble tatt per e-post eller telefon.

4.4 Oppgavens etiske side og databehandling

Denne oppgaven skal ikke publisere personopplysninger, men innehar likevel konsesjons- eller meldeplikt da det er tilfeller i datainnsamlingen hvor vi innhentet noen få personopplysninger, samt har benyttet taleopptak og lagring, og er derfor meldt inn til Norsk Senter for forskningsdata (NSD).

All førstegangskontakt med informanter ble gjort per e-post eller telefon med informasjon funnet i offentlige tilgjengelige kilder, samt gjennom ansvarlige ved de respektive virksomheter. Videre har samtlige samtykket til intervju med klar oppfordring om å ikke dele

informasjon de ikke følte seg komfortabel med å dele, samt at de ved gjentatte tilfeller ble informert om at samtykket kunne trekkes uavhengig av når i prosessen det måtte være. Samtykket ble i hovedsak innhentet skriftlig, men der dette ikke var mulig ble det tatt et muntlig samtykke etter at opptaket var startet.

All data ble anonymisert unntatt virksomhetenes navn der det var relevant og samtykket. Etter at intervjuene var ferdige, notatene renskrevet og transkriberingen ferdigstilt, ble originaldokumentene ikke endret for å ivareta validiteten gjennom dato/tid-stemplingen. Svarene ble summert opp i analysen basert på transkriberingen som vi kunne arbeide i og sammenligne data uten at vi påvirket validitetskriteriet. Oppgaven ble ikke tilknyttet noen personregistre og informantene fikk tilbud om en kopi av oppgaven etter at denne forelå ferdig godkjent (Johannesen et al., 2016, s. 83-93).

All lagring og bearbeiding av data som oppgavetekst, notater, transkriberinger og lydfiler, samt kommunikasjon med informanter ble gjort via Office365 programmene underlagt UiS domenets skytjeneste for å kunne ha god kontroll på dataene og personvernet, og på denne måten ivareta tilgjengelighet, integritet og konfidensialitet som finner i prinsippene for informasjonssikkerhet som beskrevet i teorien. Lagring av data varte frem til oppgaven ble godkjent og endelig sensur forelå.

4.5 Validitet og reliabilitet

Validitet og reliabilitet er begrep som benyttes ved evaluering og måling av kvaliteten på vår egen undersøkelse. Det snakkes om hvorvidt validitet og reliabilitet er begreper som er mer rettet mot kvantitative undersøkelser (Thurén, 2015, s 31), men de kan også brukes innenfor det kvalitative undersøkelsesfeltet, i tillegg til begreper som pålitelighet, troverdighet, overførbarhet og overensstemmelse, som i enkelte tilfeller kan være mer aktuelt for å måle kvalitet (Johannesen et al., 2016, s. 231).

For å vurdere dataenes pålitelighet, hvordan de er samlet inn og hvordan de er brukt, brukes begrepet reliabilitet. Innenfor kvalitativ forskningsmetode er det samtalene/intervjuene som i denne oppgaven styrer. Innenfor kvalitativ forskning vil ingen forsker oppnå akkurat samme resultat ettersom de forskjellige forskerne har forskjellig kompetanse og erfaring som vil lede forskningen ulikt. For å styrke påliteligheten kan forskeren gi en bedre forståelse av det

kontekstuelle gjennom en beskrivelse av oppgaven på en måte som gjør det mulig å spore innsamlingen av data og vurderingen rundt disse (Ibid, s. 231-232).

Validering brukes når troverdigheten av dataene skal måles og det skilles mellom intern validitet (troverdighet) og ekstern validitet (overførbarhet). Validitet handler om å stille spørsmål om vi måler det vi tror vi måler, sammenhengen mellom innsamlet data og det som skal undersøkes. Ifølge Johannesen et al. (2016, s. 232) er kvalitative studier ikke valide ettersom de ikke kan måles (kvantifiseres), så dette må vurderes på en annen måte. Det er fremgangsmåtene og funnene i studiene som må reflektere undersøkelsens formål og dermed representere virkelighet som avgjør om forskningen er valid eller ikke. Dette betyr at forskeren må innhente data gjennom intervjuer for så å overføre resultatene tilbake til informantene for bekreftelse eller videre analysering.

På et punkt i undersøkelsen må det vurderes om dataene kan overføres til andre forskningsområder, og ifølge Johannesen et al. (2016, s. 233) må man se på om oppgaven lykkes i å lage beskrivelser, begreper, tolkninger og forklaringer som kan være hensiktsmessig for andre områder som studeres.

For å unngå at forskerens subjektive synspunkter innenfor det faglige interesseområdet vedkommende undersøker kommer frem i oppgaven, er det med objektivitet (bekreftbarhet) meningen at forskeren fremmer et unikt perspektiv på undersøkelsen gjennom å sammenligne lignende studier for å bekrefte resultatet som andre forskere har fremmet (Ibid, s. 233-234).

4.5.1 Reliabilitet – eksempler knyttet til denne oppgaven

Først noen eksempler som er tilknyttet påliteligheten (reliabiliteten) av denne oppgavens datainnsamling. Det er relevant å gå gjennom prosessene i de ulike stadier for å vurdere om innsamlingsmetode, bruken av dataene og hvordan dataene er bearbeidet med formål om å vurdere om påliteligheten er til stede eller om den i enkelte faser kan være svak. Det var en viss fare for at kvalitativ forskningsmetode gjorde at vi kunne risikere å ikke få nok stoff til en god måling grunnet fåtall intervjuobjekter, samt tiden det tok å intervjue disse. Dog landet vi på at med et nøye og strategisk utvalg av informanter til intervjuene og hvordan vi hadde justert intervjuguiden, gjorde datainnsamlingen robust og tydelig likevel.

Oppsettet rundt intervjuene og den formelle tilnærmingen vi tok mot informantene gjorde at vi kunne etablere trygge rammer og på denne måten styrker dette reliabiliteten ved at forelå en forutsigbarhet, både i forhold til intervjuet knyttet til forskningen, men også temaet det skulle snakkes om og hvorfor det var ønske om å snakke med nettopp dem. De tilfellene hvor intervjuene foregikk via videokonferanse har blitt vurdert hvor vidt de kunne svekke reliabiliteten noe gjennom at vi mistet noe av relasjonsbyggingen med informanten, men vi vurderte at dette ikke hadde noen stor påvirkning for reliabiliteten som helhet.

Det er samtalen som styrer datainnsamlingen og vi som forskere skal kunne tolke dataene med den bakgrunn som er bygd opp, som i vårt tilfelle er stoffet vi har funnet gjennom de øvrige deler av oppgaven.

Det ble vurdert om opptak av samtalene ville medføre at intervjuobjektene ville være mer restriktive rundt hva de kunne dele, men vurderte det samtidig som bedre for oppgavens validitet og reliabilitet at dette ble gjennomført, så lenge vi sikret at dataene ikke kunne påvirkes i etterkant ved at alle lydfiler og transkriberinger fikk navn- og datomerking i tillegg til at all rådata fra intervjuene forble uendret hvor håndtering og renskrivning skjedde i egne dokumenter. Under intervjuene ble det og tatt korte stikkords notater som inkluderte tilleggsspørsmål, tips til andre kilder og forkortelser/navn som er utfordrende å hente ut fra en lydfil.

Analyseringen av dataene som ble samlet inn har kun blitt analysert av oss. Påliteligheten og verifikasjonen av de innsamlede dataene ble gjort på grunnlag av litteraturstudien og konteksten.

4.5.2 Validitet – eksempler knyttet til denne oppgaven

Videre har vi målt den interne validiteten (troverdigheten) av kildene vi har benyttet i datainnsamlingen. Vi valgte oss ut noen vinklinger ut ifra problemstillingen som har relevans for undersøkelsens formål. Vi anser det relevant å høre med ansvarlige kommunale virksomheter som per i dag står overfor risikoen for leverandørkjedeangrep. De kunne gi oss sin vurdering i henhold til sin egen organisering, risiko, leverandører og tiltak.

Videre var det aktuelt å innhente data fra fageksperter som jobbet med cybersikkerhet og informasjonssikkerhet opp mot kommunene for å få deres syn på kommunenes arbeid.

Den siste vinklingen ville vi ha fra en aktør som er organisert under et IKS for å se hvordan dette fungerer i praksis opp mot kommunene. IKS-virksomheten hadde ingen tilknytning til noen av de andre virksomhetene vi hadde med i vår studie.

Med tanke på de ulike vinklingene, de tilpassede intervjuguidene og deres tilknytning til problemstillingen/temaet, så mener vi at enhetene i datainnsamlingen er å regne som valide gitt deres ulike kompetanseområder.

I intervjuene vurderes troverdigheten som totalt sett god ved at vi tok oss god tid til møtene og intervjuguiden ikke var for omfattende. I tillegg renskrev vi notatene så raskt som mulig etter avsluttet intervju slik at det skulle være lettere å kunne komme på hva som var meningen bak stikkordene. Det er utfordrende å både intervjue og notere, men med tydelige rollefordelinger og godt forarbeid blir dataene og underlaget ansett som troverdige.

Vi har vurdert at den eksterne validiteten (overførbarheten) her er til stede ved at våre funn og forskningsmetode kan overføres til andre norske kommuner med samme problemstilling ettersom samtlige kommuner står ovenfor samme utfordring med risiko for leverandørkjedeangrep, samt hvordan risikoen kan håndteres, men det kan være at det må justeres noe i forhold til informantutvelgelsen da vi gjennom våre funn har fått informasjon om at mindre kommuner ikke har mulighet til å ha en lik organisering. I tillegg forholder andre norske kommuner seg til de samme myndighetsorganene i forhold metodeverk og styring som kommunene i denne forskningen. Når det gjelder cybersikkerhet i anskaffelser, så er funnene fra denne oppgaven direkte overførbare til både kommunale og statlige virksomheter som er omfattet av regelverk for offentlige anskaffelser.

5 Analyse

Gjennom vår problemstilling om hvordan norske kommuner håndterer risikoen for cyberangrep via underleverandørers IKT tjenester ønsket vi først og fremst å forstå hvordan kommunene arbeider med risiko for leverandørkjedeangrep med et spesielt fokus på kommunenes krav til leverandørenes IKT-tjenester under anskaffelsen og under kontraktens levetid. I de underliggende forskningsspørsmålene, ønsket vi å se på hvordan cybersikkerhet og informasjonssikkerhet blir inkludert under anskaffelsene og hvordan forholdet mellom kommunene og myndighetene er når det gjelder arbeid med risiko og cybersikkerhet/informasjonssikkerhet som to sentrale områder.

Tyngden og hovedfokuset er derfor på kommunenes arbeid med cybersikkerhet/informasjonssikkerhet og risikoen for leverandørkjedeangrep, og alle funn som er gjengitt i dette kapittelet er innhentet gjennom intervjuer med relevante informanter og stedvis gjennomgang av dokumenter og kilder etter henvisninger fra informantene. Spørsmålene vi har stilt i intervjuguiden har i hovedsak fokus på problemstillingen, mens de andre spørsmålene har et sekundært fokus mot de underliggende forskningsspørsmålene. Strukturen i dette kapittelet gjenspeiler derfor intervjuguiden slik den er oppdelt og gjennomgått med informantene innen tre hovedkategorier; risiko, cybersikkerhet/informasjonssikkerhet og anskaffelser, som også følger hovedkategoriene i henholdsvis kontekstkapittelet og teorikapittelet.

Funnene er presentert oppsummert under de forskjellige hovedkategoriene med ytterligere fordeling under disse hvor sammenligning av likheter og ulikheter er belyst. Enkelte steder er det relevant å gjengi direkte sitater hvor det henvises til et informantnummer vi har definert selv og som ivaretar anonymiteten til informanten og dens virksomhet. Vi har to virksomheter som har stilt med faglig dybde innen cybersikkerhet og informasjonssikkerhet med formål om å få en annen vinkel på spørsmålene vi stiller kommunene. Disse virksomhetene er: 1) Orange Cyberdefence som er en virksomhet i det private markedet og jobber blant annet opp mot kommuner innen cybersikkerhet/informasjonssikkerhet, og 2) kommune-CSIRT (CSIRT = Computer Security Incident Response Team), som er en virksomhet av interkommunalt samarbeid med over 50 medlemskommuner som gir rådgivning og varslingstjenester til kommunene, koordinerer erfaringsutveksling mellom medlemskommunene og inngår i NSM sitt sektorvise responsmiljø. Begge virksomhetene har samtykket til å bli gjengitt med virksomhetsnavn i denne oppgaven.

Informantene bruker stedvis forskjellig terminologi og for å kunne gjengi dem mest mulig korrekt bruker vi stedvis det som blir sagt ordrett. Av eksempler som vil komme gjennom teksten er:

- Informasjonssikkerhet/cybersikkerhet, digital sikkerhet og IKT-sikkerhet brukes om hverandre, men har samme definisjon som vist under sentrale begreper.

5.1 Informantenes stillingstitler sett opp mot bakgrunn og kompetanse

Samtlige intervjuer ble startet med å innhente noe data om informantenes stillingstittel og funksjon, og bakgrunn for stillingen/funksjonen. Vi etterspurte 3 roller for datainnhentingen; ansvarlig innen risiko, ansvarlig innen cybersikkerhet/informasjonssikkerhet og ansvarlig for anskaffelser.

Innen *risiko* så vi ingen med formell utdannelse eller tung bakgrunn, og personene som hadde denne rollen hadde en veldig ulik kompetanse- og erfaringsbakgrunn for stillingsbeskrivelsen. De personene som hadde fått en funksjon tildelt sin rolle uten å ha relevant faglig bakgrunn var derfor i større grad avhengig av kurs, veiledere, rådgivning og ekstern bistand for å kunne klare oppgavene de var tildelt.

Innen *cybersikkerhet/informasjonssikkerhet* var det en funksjon som var tillagt en rolle, og stort sett var det IKT-personell hvor kompetanse var ivaretatt gjennom utdanning og erfaring som hadde denne funksjonen. Men i noen tilfeller var det personer med annen bakgrunn som hadde fått tildelt denne funksjonen i sin stillingsbeskrivelse og disse var avhengige av veiledere, kurs og lignende for å kunne skjøte rollen.

Innen *anskaffelser* var det noe større variasjon hva gjelder relevant kompetanse for å kunne utøve funksjonen. Noen hadde veldig tung kompetanse med mye henvisning til teori og modeller som ikke gikk under de offentlig tilgjengelige veiledere og regelverk, mens andre hadde fått denne funksjonen tildelt uten stor tyngde i det, på lik linje med de som hadde cybersikkerhet/informasjonssikkerhet som tilleggsfunksjon. Hvor vidt dette var hele stillinger eller var prosentbasert, var også noe ulikt.

Informantene selv meldte at det var en svakhet i de tilfellene hvor det var funksjonsbasert og ikke en fullstendig stilling med bakgrunn innen fagområdet, og som minimumskrav for å lykkes ble det av den ene beskrevet som:

«Du må putte det på en person, gi personen ressurser og personen må være motivert for å få en god fremdrift» (Informant 5).

Samtlige informanter som stilte til intervju, var bevisste på problemstillingen og beskrev leverandørkjedene som noe de ikke hadde god nok kontroll på og etterlyste mer fokus på dette området, ikke bare innen egen virksomhet, men på generelt grunnlag med statlig initiativ.

5.2 Risiko

- **Hvordan har kommunen/virksomheten organisert arbeidet med risiko?**

«Kommuner skal i utgangspunktet være risikostyrt» (Informant 2).

Sitatet henviser til at risiko skal være tilstede i virksomhetsstyringen og alle informanter var enig i at risiko er et viktig arbeid i de kommunale virksomhetene, men vi så at det var ulik organisering, forankring og utøvelse av risikostyring/-håndtering i praksis for å få god kontroll på risikoen.

Som vi har redegjort for i teorikapittelet, er kommuner å regne som en kompleks organisasjon og komplekse systemer med komplekse verdikjeder, noe som tydelig kommer frem i dataene som er samlet inn. Det var ingen likhet i organiseringen mellom de ulike case-kommunene og i de aller fleste tilfeller hvor dette spørsmålet ble stilt, kom det ofte setninger som «vi har akkurat...», «vi skal til å...» eller «vi holder på med å...» for å vise til at de kontinuerlig jobber med å finne den ideelle organiseringen for risikoarbeidet. Dette er ikke bare gjeldende for organiseringen rundt risiko, informasjonssikkerhet/cybersikkerhet eller samspillet med anskaffelsene, men også i andre aspekter for å kunne sette en organisasjon som samhandler på tvers av avdelinger, og også andre virksomheter der det er inngått samarbeid. En av informantene beskrev det slik:

«*Det handler om å få frem og jobbe målrettet mot den reelle risikoen og til syvende og sist i kommune Norge, så handler det om to ting; kompetanse/forståelse og økonomi»* (Informant 4).

Det pekes på store variasjoner mellom kommuner, og også sektorer innenfor samme kommune, når det gjelder arbeid med risiko. Selv om det er etablert et system for risikovurdering, -håndtering og -styring på overordnet nivå, så oppleves det ulik modenhet og forståelse nedover i organisasjonen og på tvers av avdelinger/sektorer hvor det ofte fører til at det ikke gjennomføres risikovurderinger. Og i de tilfeller hvor det gjøres, blir det

hybridløsninger, manglende oppfølging og stor variasjon i risikoens alvorlighetsgrad. Mangelfull dokumentasjon ble og nevnt som en utfordring hvor det manglet system og lagring i mange av de tilfellene hvor det har blitt gjennomført en risikovurdering. De ressursene som aktivt jobber med risiko, blir i mange tilfeller ansett som et forsinkende ledd i prosessen og blir ved flere anledninger utelatt. En informant (10) som hadde risikoansvar for en avdeling i en case-kommune omtalte sin rolle som en rolle andre «hatet» på bakgrunn av at synliggjøringen av risikoen skapte merarbeid og forsinkelser, eller som informanten selv beskrev det:

«... en stor tue som velter lasset deres».

Denne skildringen var noe vi kunne se flere tilfeller av, hvor de som maste om risiko og sikkerhet ofte ble ansett som forstyrrende elementer og til dels utelatt fra viktige prosesser.

Interkommunalt samarbeid

Interkommunalt samarbeid (IKS) er noe som går igjen hos flere av case-kommunene. Et IKS er enten et interkommunalt samarbeid hvor flere kommuner går sammen for å etablere en felles virksomhet underlagt et eget styre (IKS-loven, §10), et såkalt offentligrettslig organ (anskaffelsesforskriften, §1-2), eller til tredjeparts virksomheter i det private marked som selger tjenester til den enkelte kommunale virksomhet. I denne oppgavens sammenheng har vi kommet over IKS for IKT tjenester, anskaffelser og hendelseshåndtering av digitale trusler (CSIRT).

«De kommunene som gjør det best, er de som har gått sammen og etablert IKS selskap»

Sitatet er en erfaringsbasert tilbakemelding fra Orange Cyberdefence basert på deres arbeid med kommunene. De begrunner dette med at de som inngår IKS vil ha større fokus på kjerneoppgavene og klarer å sikre bedre bestillerkompetanse på vegne av kommunene. Case-kommunene 3 hadde tjenesteutsatt sine IKT tjenester til en privat aktør, men tok driften tilbake av sikkerhetsmessige årsaker (Informant 11, 12 og 14). I et IKS er det opprettet et styrings- og oppfølgingssystem hvor hver kommune skal stille med representant, men der ser vi at flere av de oppnevnte rollene ikke har relevant bakgrunn, utdanning eller kompetanse, men at de likevel har fått tildelt en rolle som de ikke har forutsetningene for å kunne gå i dybden på. Og selv om IKS er et bra tiltak med mye god kompetanse og gode sparringspartnere, så trekker informant 10 frem at fellesanskaffelser via IKS for flere kommuner er noe som per nå ikke fungerer optimalt da det meldes inn mange behov og

ønsker, og det systemet som da blir anskaffet blir ikke tilpasset den enkelte virksomhet som det hadde gjort dersom kommunen stod alene om anskaffelsen.

IKT tjenester var noe flere av virksomhetene vi kom over hadde tjenesteutsatt. Der ansvar og databehandling forelå hos en ekstern aktør, eksempelvis hos et felles IKS eller en privat aktør, var tjenesten enten satt videre eller i ferd med å settes videre til enda en underleverandør, noe som øker kompleksiteten i databehandlerkjeden. Det var flere eksempler på dette, men et gjentagende eksempel var implementeringen av Microsoft Office 365 hvor dataene ikke lengre lå på en lokal server, men var flyttet til Microsoft sin infrastruktur. Selv om NSM ser positivt på skyløsninger fremfor intern infrastruktur, så er det flere fallgruver som en kommune må være observante på som sikkerhetsinnstillinger og gode databehandleravtaler som vi kommer tilbake til senere i oppgaven

Også når det gjaldt anskaffelser fant vi et tilfelle hvor det er inngått en avtale om et IKS hvor flere kommuner har representanter inn i en felles anskaffelsesenhet som leverer tjenester til samtlige kommuner innad samarbeidet.

Når det gjelder IKS for hendelseshåndtering er Kommune-CSIRT det eksempelet vi kom over, som og er virksomheten som stiller som fagekspert i dette studie. Denne virksomheten ble opprettet på bakgrunn av at dette var et behov kommunene så, og at det manglet et statlig insentiv på dette området. Kommune-CSIRT skal bistå kommunene med forbyggende arbeid innen digital risiko og cybersikkerhet/informasjonssikkerhet, samt fungere som et varslingsorgan ved hendelser i cyberdomenet. Kommune-CSIRT yter tjenester til kommuner som inngår i medlemsporteføljen, hvilket over 50 kommuner per nå har gjort, og finansieres blant annet gjennom medlemsavgifter og frivillighet.

Det som likevel kommer frem når det gjelder risiko innen cybersikkerhet og informasjonssikkerhet, uavhengig interkommunalt samarbeid eller intern kompetanse, er at det er noe organisasjonen, foruten IKT, anser som noe de ikke trenger å bekymre seg for da de anser det som ivaretatt av IKT ressursene uten at de kan referere til hvordan dette er ivaretatt. Flere av våre informanter viser til en stor ansvarsplassering og avhengighet til IKT-personellet grunnet manglende kompetanse.

Kommunenes størrelse og kompleksitet vil også tilsi ulikheter i forhold til tilgjengelige ressurser og kompetansegrunnlag. Mindre kommuner er mindre komplekse, men de har ikke like mange ressurser på viktige roller for å kunne jobbe med risiko på en god måte. Større kommuner kan sikre ressursene på en bedre måte, men de er og i større grad komplekse, noe

som vi ser under teorikapittelet hvor Charles Perrow beskriver at komplekse organisasjoner har større utfordringer for å jobbe med sikkerhet. Ifølge kommune-CSIRT vil kompetansen likevel være tilstede i større grad i større kommuner enn i de små.

- **Hvordan har virksomheten definert risiko?**

Definisjonen var i flere tilfeller ikke fastsatt på overordnet nivå og det var en variasjon i forhold til hva som skulle risikovurderes. I de tilfellene hvor risiko ble definert av informantene, ble det beskrevet som enkle metoder som eksempelvis «sannsynlighet X konsekvens = risiko» eller «enkle ROS modeller». Det ble henvist til standard risikomatriser i enten en 3x3, 4x4 eller 5x5 variant med fargekoding (rød, gul og grønn sone) hvorav Kommunal Informasjonssikkerhet (KiNS) sin modell ble trukket frem som et verktøy de benyttet, hvilket er en 5x5 matrise som beskrevet over (u.å). Selv om ikke alle oppga KiNS modellen, så ble det beskrevet en lik modell med de samme metodiske tilnærmingene. Det var likevel en informant som så vidt hadde begynt å jobbe med en modell som vedkommende mente ga litt mer informasjon rundt risikoen, og det var trefaktormodellen som inkluderer trusler, verdier og sårbarheter. Bakgrunnen for de lette modellene var at det måtte være lett å forstå og lese de uavhengig av hvilken risikokunnskap en besitter. Å bruke komplekse modeller uten faglig tilnærming til risikofaget ble beskrevet som utfordrende å bearbeide og vil føre til vegring, og som den ene informanten beskrev det:

«... det er og et pedagogisk element i dette» (Informant 5).

Vi fant også variasjon i hvorvidt case-kommunene hadde satt kriterier for hvordan konsekvens og sannsynlighet skulle vurderes. I de tilfellene dette var satt, var erfaringen at arbeidet med å vurdere lik risiko ble enklere selv om det også var variasjoner da akseptkriteriene var vanskelige å sette. I de virksomhetene hvor dette ikke var fastsatt var det og større kvalitative ulikheter i risikovurderingene. Det ble og henvist til flere aktører som jobber med å utvikle programvare og tilpassede risikomodeller for kommuner som noen av case-kommunene hadde inngått avtale med og var i prosess med å utvikle et tilpasset verktøy for deres virksomhet da dette var en mangelvare. Med et felles system, håpet mange av informantene at organisasjonen ville benytte systemet og at mengden av risikovurderinger, kvaliteten på dem og oppfølgingen av de ville stige markant.

Tilnærmingen til risikoarbeidet var stedvis ulik i alle case-kommunene vi hadde med i forskningen og innad samme virksomhet var det også ulikheter. Samtidig ble det i flere tilfeller trukket frem viktigheten av et langsiktig mål om et felles system, en felles definisjon,

et felles verktøy, felles forståelse av risikoelementene, felles risikoterminologi og felles metode å gjennomføre risikovurderinger basert på fastsatte kriterier for egen virksomhet.

I tabell 5.1 skisserer vi funnene våre per case-kommune.

Kommune 1	**Kommune 2**	**Kommune 3**
Sannsynlighet x konsekvens = risiko (4x4 matrise)	Sannsynlighet x konsekvens = risiko (3x3 matrise)	Sannsynlighet x konsekvens = risiko (4x4 matrise)
Enkle risiko og sårbarhetsanalyser	KiNS modellen (5x5 matrise)	Personvernkonsekvens-vurderinger (DPIA)
	Personvernkonsekvens-vurderinger (DPIA)	

Tabell 5.1 – Risikodefinisjon i de forskjellige case-kommunene

- **Benytter virksomheten et rammeverk for risikostyring?**

Som beskrevet i teorikapittelet er risiko levende og slutter ikke å endre seg etter å ha definert den. Et rammeverk for risikostyring kan bistå med å etablere kontroll ved å følge standarder, teoretiske modeller og tilpassede veiledere. Oppsummert i tabell 5.2 vises hvilke tilbakemeldinger vi fikk fra case-kommunene når vi stilte spørsmål om rammeverk for risikostyring.

Kommune 1	**Kommune 2**	**Kommune 3**
Internkontrollsystemet – «Orden i eget hus»	NSM grunnprinsipper for IKT sikkerhet	Internkontrollsystemet – «Orden i eget hus»
NSM grunnprinsipper for IKT sikkerhet	ISO 27001	SAMSVAR
ISO 27001		
Diri (cyber risiko)		
CIS20		
Norsk Helsenett		

Tabell 5.2 – Case-kommunenes rammeverk for risikostyring.

Selv om alle informantene var enstemmige i viktigheten bak risikostyringen, så meldte flertallet av informantene at det var mangelfull oppfølging av risikoen, spesielt rettet mot oppfølging av definerte tiltak for å få kontroll på risikoen hvor de ansvarlige ikke fulgte opp tiltakene. Det ble heller ikke foretatt en ny vurdering basert på ny informasjon eller innfridde

tiltak, og derfor hadde to av case-kommunene har inngått samarbeid med eksterne virksomheter innen risiko fra henholdsvis Diri og Samsvar.

Diri er et relativt nytt selskap som fokuserer på å etablere risikovurderinger og styringssystem som er tilpasset cyber og skal være enkelt å bruke samtidig som det gir kvalitative analyser. Metoden er basert på risikoforskning innen cyber fra Norges teknisk-naturvitenskapelige universitet (NTNU) og bygger på ISO 27005 standarden (Diri, u.å.). ISO 27005 er for øvrig industriens standard for risikohåndtering innen informasjonssikkerhet (Wangen, 2017, s. 133; Standard Norge, 2018).

Samsvar er en skybasert samleplattform for flere formål, deriblant en modul for risikohåndtering for informasjonssikkerhet basert på ISO 27001 som kommune 3 har begynt å bruke (informant 12; informant 14; Samsvar, u.å.).

Alle de kommunale virksomhetene vi snakket med i forbindelse med denne oppgaven, også de som har risikostyring som en del av internkontrollen på overordnet nivå, er i ferd med å revidere og lage standarder og/eller rammeverk for risikostyring som er like for hele organisasjonen da de anser dette som en sårbarhet ettersom det er ulik risikotilnærming, ulik modenhet og bruk av ulike metoder innad i organisasjonene (eksempelvis DPIA kontra KiNS modellen).

CIS20, som case-kommune 1 refererte til, er en liste med 20 anbefalte sikkerhetstiltak innen organisatorisk informasjonssikkerhet og gir eksempler på områder som en organisasjon bør fokusere på for å få en bedre rustet organisasjon og teknisk installasjon. Listen er utarbeidet av «Center for Internet Security (CIS)» tiltakene fungerer som et rammeverk for å bidra til å nå målet om å redusere fare for cyberangrep og sikre informasjon i organisasjoner. Tiltakene er vurdert som lavkost slik at tiltakene for bedre sikkerhet i mindre grad skal bli hindret av økonomiske vurderinger (Kobezak et al, 2018). CIS20 har nå blitt omdøpt til «18 CIS kritiske sikkerhetskontroller» og antall tiltak er redusert til 18 (CIS, u.å.). Kommunen hadde i dette tilfellet benyttet rammeverket som kriterier og målepunkter i sine risikovurderinger da dette fungerer til å måle gapet mellom rammeverkets beskrivelse og eksisterende oppsett, samt at de de har definerte tiltak å planlegge ut ifra (Informant 5).

Norsk helsenett er noe som står sentralt i alle kommunene og case-kommune 1 anser dette også som viktig i vurderingen av risiko gitt målekriterier med tanke på at tjenesten stiller

strenge krav til informasjonssikkerhet og risikostyring (Norsk helsenett, u.å.a) som kommunen forsøker å jobbe etter. Norsk helsenett er et statlig foretak, eid av Helse- og omsorgsdepartementet, med oppgave om å utvikle, forvalte og drifte nasjonale e-helseløsninger og infrastruktur, og med det sørge for en sikker samhandling i helsesektoren (Norsk helsenett, u.å.b). De er med å utvikle og forvalte «norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren», heretter referert til som «Normen» (Direktoratet for e-helse, 2020a, avsnitt 1.6) som de også benytter som krav til sikker bruk av sine tjenester. Normen bygger på ISO 27001 med Annex A og har en liste med 294 krav med referanser til forskjellige punkter i nevnte ISO-standard, samt relevante lovtekster (Direktoratet for e-helse, 2020b). Og det er disse kravene informant 5 henviser til. Vi vil komme tilbake til Norsk Helsenett og kravene i Normen i oppgavens analyse og drøfting.

- **Har virksomheten satt risikoakseptkriterier?**

Risikoaksepten vil være, som vi har sett i teorikapittelet, basert på hvor høy risikoen er kontra hvilke tiltak som kan settes inn, vurdert opp mot et økonomisk perspektiv. Høy risiko skal ned med kortsiktige og kraftige tiltak, middels kan håndteres med mer langsiktige og moderate tiltak og lav risiko trenger lite eller ingen tiltak. På et punkt må det vurderes at det er tilstrekkelig med tiltak og at restrisikoen anses som håndterbar. Informantene er vel forent om denne praksisen, spesielt med å få ned risikoen fra rødt nivå, men å sette akseptkriterier på middels og lav risiko viser seg å være utfordrende for kommunene. Det refereres til at dette må gjøres for hvert tilfelle og at det ikke foreligger konkrete kriterier på overordnet nivå, annet en matrisemodellen rødt, gult og grønt. I tabell 5.3 oppsummeres tilbakemeldingene fra hver case-kommune for hvilke kriterier de må ta med i vurderingen når de skal akseptere restrisikoen.

Kommune 1	**Kommune 2**	**Kommune 3**
Økonomi	Økonomi	Økonomi
Lovverk	Lovverk	Personvern
Personvern	Personvern	Liv/helse
Norsk Helsenett		Menneskelig adferd
		Restriksjoner på brukervennligheten

Tabell 5.3 – Case-kommunenes kriterier for restrisiko

Det skilles stedvis mellom praktisk og formell tilnærming til risikoaksept, hvor det på det formelle nivået er vanskelig å sette overordnede kriterier for risikoaksept, men når det gjelder det praktiske blir dette tatt som en skjønnsmessig vurdering i henhold til den prosessen de står i og kriteriene vil være ulike fra gang til gang. Noen kriterier settes på bakgrunn av lovverk som eksempelvis helse- og omsorgstjenesteloven (2011, kap. 1), sivilbeskyttelsesloven (2010, §1) eller personopplysningsloven (2018, art. 1). Vi ser og at spesielt case-kommune 1 oppgir at de benytter Normen hvor flere av kravene til informasjonssikkerhet brukes som målekriterier for egen risikoaksept.

I andre tilfeller blir overveiende tyngde lagt på økonomi da kommunene blir presset på dette området og må få mest mulig ut av tjenestene for minst mulig penger, noe som kan komme på akkord med sikkerhet da høyere grad av sikkerhet også er forbundet med høyere kost. Menneskelig adferd er også noe kommunene har vanskelig for å sette noen kriterier rundt.

Det er og veiledere og lovverk som går mot hverandre og det blir da utfordrende å finne en balanse som både ivaretar beste praksis og innenfor oppgitt lovverk. Informant 3 trakk frem et eksempel rundt dette med innføring av digitale verktøy på barneskolen for det oppstår et gap mellom utdanningsdirektoratets krav til at skolenes og oppvekstsektorens bruk av IKT for modning av elevers digitale ferdigheter, og Datatilsynets syn på risiko innen barn og digitale verktøy, og som informanten selv beskriver:

«Og da blir det et lite avvik innenfor oppvekstsektoren på hva det er greit å utsette elevene for av digital risiko fra Datatilsynets side, mens utdanningsdirektoratet sier at det er en del av læreplanen. Og så sitter man i mellom og blir litt i limbo for hva som er greit og ikke.»

Et annet eksempel er når det i forbindelse med koronapandemien ble tvunget gjennom bestemmelser for hjemmekontor/-skole for ansatte og elever hvor det måtte lettes på noe sikkerhet for å få dette til. Det blir da en økt sårbarhet og mindre kontroll, noe som kunne resultert i angrep. Det er krevende å sette noen kriterier for risikoaksept når slike eksempler tvinger frem en usikkerhet og splitt i forhold til hva som er rett. Èn case-kommune hadde en fordeling mellom sektorvis vurdering av risikoaksept som ble diskutert med kommunedirektøren i de enkelte tilfellene da de så at defineringen av risikoen måtte skje innen de respektive tilfellene med fagtilknytning og at dette måtte vurderes opp mot økonomi (Informant 11).

- **Hvordan opplever kommunen myndighetenes arbeid med risiko?**

Det er mange myndighetsorganer og definisjonen ser vi nok er noe ulik i forhold til om dette er statlige eller kommunale myndigheter da noen anså eksempelvis KS som et slags myndighetsorgan, og der ser vi at det blir en interessekonflikt.

«Alle vil deg vel, men det er ikke synkronisert, og det er ikke samkjørt» (informant 5).

Denne kommentaren oppsummerer alle informanters inntrykk. Myndighetenes arbeid skal bistå kommunene med å definere og håndtere risiko, men det finnes så mange aktører som skal jobbe med dette mot kommunene. Noe er initiert av myndighetene som eksempelvis Norsk senter for informasjonssikring (NorSiS), Nasjonal sikkerhetsmyndighet (NSM), Norsk helsenett, Digitaliseringsdirektoratet (Digdir) - tidligere direktoratet for forvaltning og IKT (Difi), og foreningen for kommunal informasjonssikkerhet (KiNS) for å nevne noen. I tillegg er det egne organisasjoner og IKSer hvor kommuner må inngå som medlemmer, ofte forbundet med en kostnad for medlemskapet. Kostnader blir også forbundet med kjøp av tjenester eller produkter som hjelper med å definere og overvåke risikoen selv når myndighetene ikke står samlet om dette, men det blir da nok en leverandør og en leverandørkjede å forholde seg til og kommunene ønsker heller at dette skal komme fra et statlig hold fremfor å måtte kjøpe tjenester ettersom økonomi er, som vi har nevnt tidligere, noe kommuner må ha et nøkternt forhold til.

Totaliteten er derfor veldig forvirrende og de generelle tilbakemeldingene fra informantene er at dette er gode virksomheter med mye bra kompetanse som ville hjulpet kommunene, som vil alt det beste for kommunene og som utgir mye god informasjon, men det er så fragmentert at det ikke er mulig å overholde kontroll over hvem som kan bistå med hva. Det etterlyses også mer ressurser fra myndighetenes side for å kunne bistå virksomhetene mer aktivt fremfor å bare prate om hva som må gjøres og stedvis henvise til hvordan det kan gjøres. Det har også kommet flere tilbakemeldinger hvor kommunene har inntrykket av at myndighetsressursene kun kommer når det skal pekes på hva som ikke er på plass ved eksempelvis ulike tilsyn, men det foreligger ingen tilgjengelige ressurser for forebyggende arbeid og bistand for å komme på akseptabelt risikonivå. Silo-virksomheter blir brukt som en benevnelse hvor informant 11 forklarer det med at myndighetsaktørene jobber kun innen egen organisasjon og ikke på tvers slik det burde for kunne yte best mulig tjeneste til kommunene.

Om en ikke sitter med dette på daglig basis, så må det mye tid til for å kartlegge og sette seg inn i dette systemet. Det samme gjelder føringer som kommer inn fra alle kanter, eksempelvis

fra Statsforvalteren, direkte fra bistandsaktørene som nevnt over og via medlemsorganisasjonene kommunene er medlem av. Det etterlyses mer bevisstgjøring av risikoområdet for å skape en felles forståelse av hva risiko er, hvordan risiko kan håndteres og hvordan leve med risiko, samt mer fokus fra styrende myndigheter for å kunne få råd, tips og veiledning for hvordan kommunene skal håndtere risiko i en mer strukturert og forstått form ettersom dette er ting de per i dag ender opp med å søke gjennom egne medlemskap da det blir for komplekst å håndtere internt.

Innen IKT risikoarbeidet ble NSM i flere tilfeller trukket frem som en aktør som virksomhetene har stor tillitt til og case-kommunene benytter mye av deres fagstoff inn mot eget risikoarbeid.

5.3 Cybersikkerhet

- **Hvordan har virksomheten organisert arbeidet med cybersikkerhet?**

Rett organisering med relevant kompetansekrav vil være en faktor for å kunne jobbe med cybersikkerhet og informasjonssikkerhet på overordnet nivå, og sammensetningen hos case-kommunene er noe ulik i forhold hva de selv mener er viktig å ha med innen tematikken. Likevel er det noen roller som går igjen som fellesnevnere, hvilket er ansvarlig innen informasjonssikkerhet, databehandling, ansvarlig for personvern og representant fra IKT, samt samarbeid med eksterne aktører som Digi Viken (partnerskap mellom kommunene og Viken fylkeskommune innen digitalisering) som i flere tilfeller inngår i case-kommunenes organisering for cybersikkerhets- og informasjonssikkerhetsarbeidet.

Men i mange tilfeller blir miljøene små, noe som Orange Cyberdefence peker på som problematisk da det blir veldig rolleavhengig. Og om ressursen innen eksempelvis cybersikkerhet/ informasjonssikkerhet blir borte, så har det stor innvirkning for kommunen. Orange Cyberdefence ser med fordel om det dannes egne sikkerhetsavdelinger i kommunene med god tverrfaglig risiko- og sikkerhetskompetanse for å kunne sikre god bestillerkompetanse innen flere sikkerhetsområder, samt god redundans ved fravær. I tabell 5.4 lister vi opp hvilke roller case-kommunene definerer som viktige i arbeidet med cyber- og informasjonssikkerhet.

Kommune 1	Kommune 2	Kommune 3
Ansvarlig informasjonssikkerhet	Ansvarlig informasjonssikkerhet	Ansvarlig informasjonssikkerhet
Fagansvarlig IKT og IKT sikkerhet	Interkommunalt samarbeid - IKT	Fagansvarlig IKT
Personvernombud	Ansvarlig personvern	Ansvarlig personvern
Endringsutvalg (gruppe som behandler avtaleendringer og anskaffelser)	Sikkerhetsansvarlig	Digi Viken
		Systemforvalter sky

Tabell 5.4 – viktige roller i case-kommunenes organisering for cyber-/informasjonssikkerhet.

Men selv om de oppnevnte rollene er viktige ressurser innad arbeidet med cyber- og informasjonssikkerhet, så er kulturen blant medarbeidere et område informantene legger stor vekt på. God sikkerhetskultur krever konstant oppfølging, og det pekes på veldig ulik modenhet innad i organisasjonen når det gjelder teknologi og sikkerhetsforståelse, noe som gir en utfordring i bevisstgjøringen. Men helsearbeidere og IKT fagressurser blir ved flere anledninger trukket frem som jevnt gode på cyber- og informasjonssikkerhet. Dette begrunnes med regulerende lovverk, samt at dette er en del av utdanningen deres. Så kunnskap og forståelse om at den informasjonen de besitter må beskyttes gir et godt grunnlag for god kultur innen cyber- og informasjonssikkerhet.

Det samme gjelder når det skilles mellom store og små leverandører, da mindre kontrakter får mindre fokus og oppfølging enn større kontrakter og rammeavtaler, samt at det også her pekes på lovverk i enkelte sammenhenger som sikrer gode tiltak mot cyberangrep. Sikkerhet i alle ledd er viktig for å unngå cyberangrep og flere av informantene nevner nettopp dette, og at det er viktig å inkludere leverandørene i arbeidet. Kompetanse, rammevilkår og forutsetninger blir pekt på som viktige faktorer for å skape forståelse av oppgaven en er satt til å forvalte, og der må cyber- og informasjonssikkerhet inn. Det oppleves at cyber- og informasjonssikkerhet får altfor lite fokus og for lite ressurser på begge sider av leverandørkjeden, noe som gjør oppfølgingen begrenset (Informant 9).

Det er og en endring i markedet som gjør at leverandørene går mer over til skyløsninger fremfor lokal server, noe som betyr en endring innad leverandørkjeden som må tas med i

arbeidet. Selv om skyløsninger blir vurdert som en sikrere løsning av NSM, Orange Cyberdefence, Kommune-CSIRT og andre cybersikkerhetsaktører, så må det fremdeles foreligge en forståelse om hva dette innebærer og hvordan risikobildet endrer seg.

For å håndtere cyberangrep, som i alt annet ved beredskapsarbeid, følges prinsippene ansvar, likhet, nærhet og samvirke og her ser vi at kommunene i stor grad lener seg på interkommunalt samarbeid som utsatt IKT-tjeneste og hendelseshåndteringstjenester. Orange Cyberdefence har og den generelle oppfatning om at kommuner misforstår hendelseshåndteringstjenestene (CSIRT) da de forventer en aktiv håndtering i egen virksomhet for å hjelpe virksomheten opp igjen, men i realiteten vil de kun fungere som en varslingsenhet ut mot andre risikoberørte virksomheter, dette er noe også Kommune-CSIRT understreker hvor de ikke aktiv går inn og håndterer hendelser i sine medlemskommuner. Slike hendelseshåndteringsteam er i tillegg ikke et statlig organ rettet mot kommuner og det opereres derfor med egen organisering, medlemskap og kjøp av tjenester for å ruste egen virksomhet ved slike hendelser. Orange Cyberdefence mener kommuner er bedre rustet om de organiserer slike team internt med relevant kompetanse og kunnskap som en forlengelse av beredskapsorganiseringen, og stedvis etterlyser og informantene innad case-kommunene en organisering som tilligger beredskapsledelsen.

I analysens risikodel så vi at det var en kultur for å ha tillit til at IKT-ansvarlige hadde kontroll på all digital risiko, men vi ser også at en av case-kommunene har tillagt sin IKT-avdeling å håndtere digitale og personvernmessige problemstillinger og hendelser i sin organisering slik at alle saker som meldes oppover i linjen blir videre sendt til denne gruppen. De har og høyere beslutningsmyndighet og oppståtte hendelser og problemstillinger blir derfor løst raskt og «lite byråkratisk» (Informant12).

- **Benytter kommunen/virksomheten et rammeverk eller standard for cybersikkerhet?**

Et rammeverk eller en standard for cybersikkerhet/informasjonssikkerhet kan variere og vil reflektere hvilken informasjon som ligger tilgjengelig for case-kommunene ettersom det ikke ligger en dyptgående kunnskap om dette i de virksomhetene vi har vært i dialog med. De som kunne svare opp disse spørsmålene var utelukkende noen få med IKT kompetanse og informasjonssikkerhetsansvarlige, mens resterende som fikk samme spørsmål ikke kunne svare, men henviste til tillitt og avhengighet av det personellet som kunne noe om det. Det

rammeverket eller de standardene som informantene nevnte at de benyttet, eller var i ferd med å benytte står listet i tabell 5.5.

Kommune 1	**Kommune 2**	**Kommune 3**
Norsk Helsenett – Normen	Norsk Helsenett – Normen	Norsk Helsenett – Normen
ISO 27001 (oppstartsfase)	ISO 27001 (oppstartsfase)	NSM grunnprinsipper for IKT sikkerhet
NSM grunnprinsipper for IKT sikkerhet	NSM grunnprinsipper for IKT sikkerhet	Internkontrollsystemet – «Orden i eget hus»
CIS 20		SAMSVAR
Diri (cyber risiko)		

Tabell 5.5 – case-kommunenes forhold til rammeverk/standard for informasjonssikkerhet.

Alle de kommunale virksomhetene i denne studien informerer om at de har innført, eller er i ferd med å innføre NSMs grunnprinsipper for IKT sikkerhet da disse er lett tilgjengelig og tilbyr et kvalitetsstempel, samt at det vil være enkelt å videreformidle disse til andre parter i motsetning til ISO 2700-serien. Prinsippene blir og beskrevet som krevende å forvalte gitt omfanget, men samtidig enklere enn ISO 2700-serien. NSM skriver selv at deres grunnprinsipper er et supplement til andre standarder, men samtidig bygger på ISO 27002-standarden hvilket er beskrevet som et tiltaksrammeverk fremfor et styringsrammeverk hvor ISO 27001 blir trukket frem som mer relevant (NSM, 2020b, s. 8).

Alle case-kommunene benytter rammeverket fra Normen i forbindelse med bruk av Norsk Helsenett hvor de må innfri en rekke krav som beskrevet i analysens risikodel. Case-kommune 2 og 3 trekker også frem at de strenge kravene gir dem en overførbarhet til andre områder innen cyber- og informasjonssikkerhet.

I flere av case-kommunenes «... vi er i ferd med å...» kommentarene blir ISO 2700-serien trukket frem som et langsiktig mål, men per nå er det enklere å implementere NSM grunnprinsipper for IKT sikkerhet. Kommune-CSIRT sin generelle oppfatning er at deres medlemskommuner forholder seg til NSM sine grunnprinsipper for IKT sikkerhet, men at noen få har begynt å se på ISO 27001 og ISO 27002 standardene både internt i kommunen og som krav til sine leverandører. Orange Cyberdefence som sitter på privat side og ser utlysningene har så langt ikke sett noen krav til ISO-standarder, så dette mener de i tilfelle er i oppstartsfasen, noe vi får bekreftet i case-kommunene hvor de enten er i oppstartsfasen eller har et langsiktig mål om å innføre ISO 27001/27002.

Ettersom flere og flere systemer som kommunene benytter går over til skyløsninger, blir det også her trukket frem at det skal settes søkelys på en egen strategi internt i kommunene i tråd med NSMs anbefalinger (2020e) og Kommunal- og distriktsdepartementets strategi for skyløsninger (2016).

Kommune 1 har i denne sammenheng brukt CIS20 rammeverket for å verifisere og måle sikkerheten av egen infrastruktur og organisasjon i flere tilfeller og forsøker å overføre det til flere områder (Informant 5).

Case-kommune 1 (Diri) og case-kommune 3 (Samsvar) oppgir at de i denne sammenheng benytter sine kjøpte systemer for å finne tiltak for god cyber- og informasjonssikkerhet. Systemene er tilpasset dette området, og fungerer både for å avdekke og håndtere risiko i tillegg til å finne adekvate tiltak og dermed fungerer som et tilpasset rammeverk.

- **Er det gjort spesifikke tekniske og organisatoriske tiltak for å forhindre cyberangrep?**

«Vi har 50 medlemskommuner, og da er det 50 måter å gjøre det på» (Kommune-CSIRT).

Alle kommuner har ulike måter å jobbe på selv om vi ser flere likheter. Dog har vi hatt et begrenset antall kommuner i denne forskningen, mens kommune-CSIRT jobber mot flere, så det er kanskje større forskjeller ut i kommune-Norge.

Administrative tiltak:

Case-kommune 1 og 2 viser til Statens Standardavtaler (SSA) som avtaletekst. Som vi har gjennomgått tidligere, så har disse avtalene standardisert tekst om at leverandøren skal gjøre forholdsmessige tiltak for å ivareta krav til informasjonssikkerhet, som også gjelder leverandørens underleverandør (DFØ, 2019a, s.10; DFØ, 2019b, s. 28). Teksten er ikke veldig spesifikk på hvordan leverandørene skal sikre dette foruten at det stilles krav til dokumentasjon av tiltakene, og kommunene er da selv pliktig til å utforme tydeligere krav til sikkerhet og sertifiseringer (DFØ, 2021b, s. 33). Vi fikk ved et tilfelle innsyn i et avtaleutkast med grunnlag i en Statens Standard kjøpsavtale (SSA-K) hvor virksomheten, som en del av et IKS, hadde videreutviklet standardoppsettet og definert en rekke krav til sin leverandør om gjeldende lovkrav, ytterligere spesifiseringer mot personvernforordningen, informasjonssikkerhet, dokumentasjon og ISO 27001 (informant 13).

Statens standardavtaler peker og på krav til at leverandøren skal ha rutiner for sikkerhetskopiering, noe Orange Cyberdefence peker på som en generell svakhet hos

kommunene da det enten ikke eksisterer, eller har veldig reduserte sikkerhetskopieringsprosedyrer. Cyberangrepet mot Østre Toten er et eksempel hvor det ikke fantes gode sikkerhetskopier, noe som betydde at de mistet mye verdifull data når de skulle bygge opp infrastrukturen på nytt. Å bygge opp en ny infrastruktur og sette opp systemene på nytt uten dataen har vist seg å være veldig tid- og ressurskrevende.

Databehandleravtaler har det også blitt et forhøyet fokus på, og case-kommunene informerer om det stort etterslep som må tas igjen. Leverandørkjeden er det flere som nevner at de er i ferd med å ettergå med tanke på å sikre egen informasjon som de forvalter, samt gode varslingsrutiner ved hendelser og/eller endringer.

Organisatoriske tiltak:

Av organisatoriske tiltak ser vi at kommunene har startet opp og gjennomfører jevnlig bevisstgjøringskampanjer hvor sluttbruker, altså den enkelte ansatt, blir mer bevisst på lenker i e-poster med tanke på phishing-forsøk. Det er noe forskjell mellom kommunene på hvor vidt dette kun gjøres gjennom informasjonsformidling eller om det kjøres simulerte angrep i tillegg slik at det skal være en virkelighetsforståelse bak dette. Phishing-angrep er noe som Orange Cyberdefence og kommune-CSIRT, i likhet med det skisserte digitale trusselbildet vi så på i kontekstkapittelet peker på som den mest aktuelle for norske kommuner da dette er metoder som er enkle og som bygger på tillitsforhold. NSM (2021a, s. 17-20) peker på at dersom en leverandør blir angrepet og trusselaktørene kommer seg inn der, så vil tillitsforholdet mellom leverandør og kunde være veien inn i kommunenes infrastruktur. Phishing er en metode for innsamling av eksempelvis påloggingsinformasjon (brukernavn og passord) som trusselaktørene vil kunne benytte for å komme seg inn i systemet uten å bli oppdaget. Om en bruker med mye rettigheter oppgir sin informasjon, så vil trusselaktøren få tilgang til mye informasjon og kan i verste fall ta kontroll over virksomhetens infrastruktur.

Foruten organisatorisk fokus på phishing, så ser vi og stedvis at det jobbes med å definere hva av informasjon som skal lagres hvor basert på gradering og åpenhet. Det blir stilt strengere krav til sikker lagring enn tidligere og det har blitt etablert rutiner og systemer for fillagring. Det større verktøyene, programvaren og systemene som blir benyttet har nå strengere krav til sikkerhet, men informantene opplever at de mindre programmene og systemene ikke får like strenge krav. På tross av disse organisatoriske tiltakene, så er den generelle tilbakemeldingen at forståelsen og kunnskapsgrunnlaget hos sluttbrukere og leverandørene er for lav. Kommune-CSIRT nevner og fakturasvindel som de har hatt mange saker på, men ingen av

informantene våre i denne studien peker på dette som en trussel, ei heller noe da har etablert tiltak mot.

Tekniske tiltak

Av tekniske tiltak inngår også system for sikker lagring. Dette er systemer som har en høyere grad av sikkerhet for å unngå data på avveie. Foruten dette, så ser vi at samtlige case-kommuner har, eller er i ferd med å implementere Microsoft Office 365 og går mer over til skybaserte løsninger fremfor egne servere. Microsoft Office 365 har flere pakkeløsninger på entrepriseniv å og sikkerhet er ulikt løst på de forskjellige lisensene. E5, som er den lisensen som tilbyr best sikkerhet, er også en dyr lisens. Så som informant 5 beskrev det i en kommunal økonomisk problemstilling:

«Vi blir jo prioritert opp mot barnehager, sykehjemsplasser og brukernære tjenester, så politikerne må si noe om vi skal bruke 2 millioner på å redde en barnehage eller om vi skal bruke 2 millioner på Microsoft lisenser».

Informanten beskrev det som en veldig tung interessekonflikt, men etter at Østre Toten gjennomgikk et cyberangrep blir Microsoft lisenser prioritert, og informant 11 opplever at det ikke bevilges penger til digital sikkerhet med mindre en kan vise til slike hendelser. Case-kommune 3 jobbet aktivt med Microsoft sin sikkerhetsløsning for sine digitale verktøy hvor graden av sikkerhetsnivået vurderes ut fra oppnådde poeng per innførte tiltak og virksomheten hadde klart å nå en score på 83% av 100% mot snittet som lå på 56% for tilsvarende virksomhetsstørrelser.

Drift versus sikkerhet er noe vi ved flere anledninger kom over under våre intervjuer. Manglende sikkerhet kan felle driften, men likevel melder informantene at drift alltid er prioritert før sikkerhet. Kommune-CSIRT presiserer at tilgjengelighet, som er et mål for driften, også er et av de tre hovedprinsippene for sikkerhet, så hvorfor ikke kjøre denne prosessen parallelt? Likevel erfarer de at sikkerhet er noe kommunene vurderer i ettertid, og da til en vesentlig høyere kost.

Allerede eksisterende teknisk sikkerhet er gjennomgått og forsterket ved hjelp av eksterne leverandører og ved bruk av rammeverk for kvalitetssikring av IKT sikkerhet som eksempelvis CIS20 som vi har sett på tidligere. Virksomhetene informerer om at de har hatt gjennomgang og endret systeminnstillinger, aktivert to-faktor pålogging, gjennomgått og forsterket brannmurer, fjernet gamle filservere, flyttet data til sky og strammet inn på

tilganger og protokoller for løsningene. Det er også gjort en omfattende jobb med å legge på mer digital sikkerhet og få mer kontroll på hva som tilkobles nettverket etter en lang periode med hjemmekontor/-skole som har pågått under koronapandemien.

- **Hvordan opplever du myndighetenes rolle når det gjelder forebyggende arbeid innenfor cybersikkerhet?**

«Med mindre det er lovbestemt, så kan kommunen gjøre som de vil, og det betyr jo at veldig mye av det som kommer fra sentrale myndigheter, det kan være nasjonal sikkerhetsmyndighet, det kan være digitaliseringsdirektoratet og så videre, blir en anbefaling, og det gjør at kommunen kan gjøre mer eller mindre som de vil.» (Kommune-CSIRT).

Betydningen bak utsagnet blir også etterlyst hos noen informanter, da de beskriver kommunene som altfor selvstyrte og at strengere krav til kommunene med fordel kan innføres.

Selv om det de senere årene har kommet flere verktøy og veiledere, så blir det ikke presentert som et krav som kommunene må følge, men blir en anbefaling og mer som en «trend» ved at en kommune følger NSMs grunnprinsipper for IKT sikkerhet, så derfor følger andre kommuner også de samme prinsippene. Kommune-CSIRT presiserer at eksempelvis NSM ikke har noen myndighet til å pålegge noe ovenfor kommunene og kan bare komme med råd og veiledninger. De opplever dog at Statsforvalterne følger opp og stiller krav til IKT-sikkerhet hos kommunene, og Statsforvalteren i Innlandet blir trukket frem som en som jobber aktivt på dette området. Men med krav og anbefalinger, så kommer også økt kostnad og noen peker på at det sammen med anbefalinger til bedre IKT-sikkerhet og krav til utbedring bør komme med økonomiske midler da budsjettene allerede er satt og overgått.

«Jeg vet egentlig ikke hvordan myndighetene jobber» (Informant 14).

Dette er et sterkt utsagn når det gjelder myndighetenes rolle inne cyber- og informasjonssikkerhet, og igjen blir det pekt på et sammensurium av aktører som ved samme utsagn som «vil deg vel» (informant 5). Dette utsagnet representerer alle de case-kommunene som vi har deltatt i denne studien, men vi opplever en til dels motpol fra kommune-CSIRT hvor de presiserer at dette ikke er vanskelig å forholde seg til og at dette er det deres 50 medlemskommuner også melder. Informant 5 lister opp for oss hvilke aktører de per nå som jobber med cyber- og informasjonssikkerhet mot kommunene:

«Du har Datatilsynet, du har Digitaliseringsdirektoratet, du har NSM, du har KiNS, du har Normen, du har NorSIS, du har DSB, du har DFØ, du har KS, du har UDI, du har Norsk helsenett og du har kommune-CSIRT».

Det etterlyses en tydeligere struktur og en sentral aktør som kan utfordre leverandørbransjen på vegne av kommune-Norge, noe som støttes av Orange Cyberdefence som peker på at det ikke er noen som passer på sikkerheten ovenfor leverandørene og kommunen selv må sikre dette i de aller fleste tilfeller. Unntaket blir igjen lovmessige krav som må oppfylles, eksempelvis i henhold til sikkerhetsloven, personopplysningsloven og lignende. I tillegg etterlyses det at medlemskap i offentlige virksomheter som skal bistå kommunene bør opphøre og heller støttes statlig.

«Vi trenger ikke å få den samme informasjonen 3 ganger og betale for det attpåtil» (Informant 11).

Det har og blitt pekt på uforholdsmessige krav til kommunene når det gjelder å vurdere sikkerheten og risikoen i forbindelse med krigen i Ukraina i brev fra Kommunal- og distrikts departementet, datert 9. mars 2022. Informant 2 fra IKS virksomheten stusser over at dette ikke gjøres på statlig hold som har ressurser og kompetanse til dette fremfor å dytte ansvaret over til kommunene. Kommunene har ikke kompetanse til å vurdere dette og det burde kommet noen føringer på hva som skal vurderes. Vi har funnet dokumentet det er henvist til og klipper inn avsnittet informanten reagerer på:

«Flere leverandører av programvare har utviklings- og supportavdelinger i landene som nå er involvert i konflikten. Verifiser med leverandør om hvordan leverandøren håndterer situasjonen hvis de har utviklings- eller supportavdeling i de aktuelle landene.» (Kommunal- og distrikts departementet, 2022).

Informanten synes resten av innholdet i brevet tilbyr en god sjekkliste over tiltak kommunene bør avsjekke eller implementere, og at vurdering av leverandørkjeden utenfor Norge og i krigsrammede land med hvilken risiko dette innebærer er svært viktig, men informanten presiserer at dette bør være en vurdering som tas på nasjonalt hold og formidlet til kommunene fremfor at de skal gjøre individuelle vurderinger. Det samme gjelder situasjonsbilde innen cybersikkerhet som er under konstant endring og hvordan virksomhetene skal kunne endre seg i samme takt, og der må statlige aktører kunne bistå i mye større grad enn de gjør per i dag. Og for å sitere informant 6:

«Vi hadde røvere tidligere også. Vi hadde sjørøvere, landeveisrøvere, togrøvere, og idag har vi cyberrøvere».

Myndighetene er generelt fraværende også her med unntak at vil fungere som et varslingsorgan mot berørte virksomheter. Så ved en cyberhendelse i en virksomhet, så vil aktuelle myndighet kun ha en varslingsfunksjon mot tilsvarende virksomheter som kan ha den samme sårbarheten før de igjen oppleves som passive for kommunenes del.

Og skulle kommunene bli offer for et cyberangrep, så står de egentlig med egen organisering for å håndtere hendelsen – der er ikke myndighetene og det kunne vært en tanke å få en styring og kontroll for å få til et bedre samvirke mellom kommuner og stat og/eller et felles overvåknings- og hendelseshåndteringsorgan som jobber på nasjonalt nivå og kan jobbe med kommunene fremfor å kun fungere som et varslingsorgan via et betalt medlemskap eller som kun kommer inn ved større hendelser. Orange Cyberdefence har en opplevelse om at mellomstore og større kommuner har bedre forutsetninger for å kunne jobbe med dette kontra mindre kommuner gitt organisering og økonomi, dette blir og trukket frem av informant 2, informant 11 og informant 14.

5.4 Anskaffelser

- **Hvordan har kommunen/virksomheten organisert arbeidet med anskaffelser?**

Det er mye likheter i grunnorganiseringen for anskaffelser i case-kommunene i denne oppgaven. Alle legger frem at eierskapet skal ligge hos behovshaver, ofte en leder for en sektor (eksempelvis skolesektoren), som også i mange tilfeller blir satt som prosjektleder. Det innmeldte behovet vil bli vurdert før det går til virksomhetenes innkjøps- eller anskaffelsesenhet som enten ligger internt i kommunen, eller som fungerer som en felles innkjøps-/anskaffelsesenhet for flere kommuner (IKS) hvor de får bistand og rådgivning. Prosjektleder skal videre da organisere seg med relevante ressurser for å danne kravspesifikasjon, tidslinje og kostnadsbilde, og de ressursene vi ser går igjen, foruten relevant fagperson for anskaffelsen, er personvernombud, informasjonssikkerhetsansvarlig, IKT-ressurs(er) og IKS-virksomheter der det er relevant. Her ser vi ulikheter ved at disse rollene blir tatt inn til ulike tider og ved flere tilfeller for sent med tanke på å få definert krav tidlig i prosessen, og det samme når det gjelder risiko hvor de på overordnet nivå har lagt inn en prosess for gjennomførelse og styring av risiko, men ser at dette faller stedvis bort nedover i organisasjonen slik at de ikke har kontroll på eget risikobilde innad knyttet til anskaffelsen.

Orange Cyberdefence anser dette som problematisk, også på bakgrunn av egen erfaring når de har snakket med IKT ressurser i kommuner hvor det kommer frem at det er leverandøren selv som definerer det sikkerhetsmessige uten at kunde blir inkludert fordi det ikke er stilt krav til det i anskaffelsen, til dels fordi IKT ressursene ikke er med i anskaffelsen eller fordi de kommer for sent inn. Som vi har kikket på tidligere, så må relevante ressurser tidlig inn i en anskaffelse for å kunne definere risiko og krav til leverandøren, og vi ser at det å inkludere sikkerhet i anskaffelsene er noe som er forholdsvis nytt og har først kommet med de siste årene. Informant 14 henviser til at de benytter juridisk bistand i anskaffelser tilknyttet større kontrakter, men foruten det har ikke juss vært tema i case-kommunenes organisering for anskaffelser.

Vi finner også en differensiering mellom store og ofte felles anskaffelser for flere sektorer og/eller kommuner og mindre anskaffelser som isolert sett er tiltenkt en enkel enhet. Det blir lagt mye fokus og allokert mer ressurser til store anskaffelser for å ivareta riktige krav, mens det i mindre anskaffelser blir tillagt mindre ressurser og kontroll. Det samme gjelder IKS virksomhetene hvor de ofte er tungt inne i de store prosessene, men ser også at de uteblir ved mindre anskaffelser (Informant 13; Informant 6; Informant 3). Noen case-kommuner har definert innsats basert på terskelverdier og vi ser at denne anskaffelsesverdien varierer fra under 100 000,- til 500 000,- før anskaffelsesenheten kobles inn, og anskaffelser under disse terskelverdiene blir tillagt mindre kontroll, krav og styring (Informant 6; Informant 3). Orange Cyberdefence får stadig henvendelser fra kommuner som har behov for økt sikkerhet, men opplever at de ikke får det de trenger under den nedre terskelverdien på 100 000,- for å unngå anbud og de kan derfor ikke benytte direkte anskaffelser.

Ved store anskaffelser til flere kommuner gjennom et IKS, så referere informantene til en felles innkjøpsordning hvor hver kommune må stille med en eller flere representanter. Hvilke roller representantene skal inneha er noe ulikt mellom case-kommunene vi har intervjuet da de har forskjellige interkommunale samarbeid innen anskaffelser. Der det er etablert et interkommunalt samarbeid innen IKT, vil en anskaffelse av en programvare også være ment for de andre kommunene. Office 365 er et nevnt tilfelle hvor samme system skulle anskaffes til mange medlemskommuner, hvor hver kommune måtte stille med relevante og faglige ressurser.

Kommune-CSIRT blir ved enkelte tilfeller kontaktet med forespørsel om å bistå i en anskaffelse, men de legger seg på et nivå hvor de yter enkel vurdering i henhold til eksempelvis NSM grunnprinsipper for IKT sikkerhet, men utover det skal de ikke ha en tung og avgjørende rolle i anskaffelsen og frastår fra alt kommersielt da dette ikke tilligger dem å ha en mening om.

«Har vi en trussel, så blir det ofte slik at løsningen på trusselen kan skape ny trussel. Det er dessverre sånn at vi egentlig ikke ferdig når anskaffelsen gjort, det er da vi egentlig begynner - selv om vi er forberedt godt underveis i en sånn prosess» (Informant 9).

- **Hvordan gjennomfører virksomheten anskaffelser?**

Økonomi og behov er sentralt i alles tilbakemeldinger hvor det må beskrives og vedtas et faktisk behov og sikres finansiering før prosessen blir vurdert og startet. Økonomi er som tidligere nevnt, svært viktig i kommunenes hverdag og det er ofte tunge avveininger på hva som kan benyttes av penger da budsjettene er stramme. Informant 6 fortalte om opplevde prosesser hvor anskaffelsen gikk så langt som til kontraktsignering før behovshaver kom med at det ikke forelå finansiering til anskaffelsen, noe som er uforholdsmessig med tanke på hvor mye ressurser og tid som blir nedlagt i en anskaffelse.

Selve prosessen følger anskaffelsesregelverket og her var samtlige enige om prosessen og ved et par anledninger ble det henvist til prosessen som direktoratet for forvaltning og økonomistyring (DFØ) har etablert gjennom Anskaffelser.no, se figur 5.1.

Figur 5.1 - Anskaffelsesprosessen – tid, påvirkning og kostnader (DFØ, u.å.)

Denne modellen kan sammenlignes med prosessbeskrivelsen i teorikapittelet hvor påvirkningskraften er størst i begynnelsen og synker gradvis ettersom prosessen går videre og det er her de tydeligste forskjellene rundt organiseringen og hvilke roller som kom inn når lå. Det var lettere å få inn relevante roller inn tidlig nok på de store anskaffelsene da disse fikk et høyere fokus grunnet størrelse og omfang, men må de mindre anskaffelsene var det ofte at ressursene og vurderingene rundt sikkerhet og risiko uteble eller kom for sent inn, og dermed ikke hadde noen påvirkningskraft. Orange Cyberdefence presiserer at krav til leverandørenes cyber- og informasjonssikkerhet må inn tidlig i prosessen uavhengig anskaffelsens størrelse og omfang. Om ikke dette gjøres, så vil det være en unødig stor risiko, samt at det blir vanskelig og ofte mer kostbart for kommunene å få dette inn i ettertid. Det kom der flere erkjennelser fra informantene om at de ikke var gode nok på dette, men at det var i ferd med å snu.

Differensieringen på terskelverdien blir skiltet av noen av informantene som et problemområde hvor det ligger mye ukjent risiko ettersom det ikke tillegges like mye fokus og informant 5 viser til hendelser hvor de plutselig kommer over enn applikasjon eller et system som er anskaffet under terskelverdi på 100 000,- og som skal innføres uten at relevante ressurser har vært involvert. På det stadiet er kontrakt med vilkår allerede undertegnet og påvirkningskraften blir enten borte eller veldig kostbar når det viser seg at dette er en risiko som kommunen ikke kan akseptere, og noen tilfeller har de vært nødt til å stoppe prosessen (Informant 5; Informant 11; Informant 14), eller at systemet ikke lar seg integrere i virksomhetens infrastruktur. Dette fenomenet blir også omtalt som skygge-IT og oppstår når personer eller avdelinger tar i bruk programvare, nettjenester eller kjøper produkter tikoblet nett (Internet of Things - IoT produkter) på eget initiativ for bruk i jobben uten at IT/IKT-avdelingen er involvert, eller i det hele tatt er kjent med at tjenesten/produktet anskaffes (Øyvann, 2014).

- **Hvordan vil du beskrive bestillerkompetansen ved anskaffelser med fokus på cybersikkerhet?**

God bestillerkompetanse blir pekt på som en utfordring av flere informanter, og da ikke med tanke på eget fag, men ettersom kommuner må forholde seg til en enorm faglig bredde blir det veldig variabelt nedover i kjeden med frafall av det sikkerhetsmessige, og som informant 3 beskriver det:

«Kommuner har veldig få organisasjonsledd som jobber overordnet, så de er i grøten på hver sin tue hele veien».

Som vi har sett i de case-kommunene vi har snakket med, så skorter det ikke på kompetanse i forhold til hvilke IKT sikkerhetskrav de skal stille leverandørene, men denne kompetansen ligger hos egne fagressurser som i altfor mange tilfeller uteblir fra innkjøp og anskaffelsesprosesser, spesielt de små. Det samme gjelder skygge-IT hvor de som kjøper systemer og produkter uten å besitte rett kunnskap om hvilke krav som må oppfylles, så oppstår det et sikkerhetshull og en usikker risiko som må håndteres, og som genererer mye ekstraarbeid.

«Det som ikke er så bra, er jo på sikkerhets delen med krav til utstyr, krav til leverandører, krav til underleverandør av leverandør og den type ting mener vi i utgangspunktet de ikke er så gode som de bør være. Og da er det helt generelt, og så har du de samme sprikene fra små kommuner til store kommuner» (Kommune-CSIRT).

Orange Cyberdefence har opplevd dialoger med leverandører som forteller om sin sikkerhet og kryptering hvorpå avtaleeiere i kommuner har lite kunnskap om hva det faktisk innebærer og står da med en skjult risiko. De må rustes til å kunne spørre etter hva slags sikkerhet, hvilken kryptering, om finnes det sertifiseringer og lignende, og faktisk forstå hva svarene betyr. Kommunene peker selv på at dette er en prosess de ikke har kommet langt nok i og flere nevner at det må rettes søkelys på dette området for å sikre at leverandørene blir kravstilt kvalitativt når det gjelder sikkerhet.

«Jeg visste jo ingenting om anskaffelse før jeg plutselig var i referansegruppen til et skoleadministrativt system. Jeg vet mer nå, men jeg sliter med konsekvensene av at det ikke ble ikke spurt etter de rette tingene i anbudsprosessen for skoleadministrativt system den dag i dag.» (Informant 10).

Informanten bak sitatet opplevde å sitte uten kompetanse for å kunne vurdere risiko tilknyttet systemet, og selv om vedkommende lærte mye av prosessen, så manglet rett kompetanse og forutsetningene for å kunne vurdere systemet. Informant 4 forteller om en prosess hvor læringskurven var bratt og inngående kunnskap var liten hvor de var avhengig av annen kompetanse for å få god sikkerhet og minimert risiko.

Den generelle bekymringen vi finner ligger ikke på de som til daglig jobber med anskaffelser eller IKT, men de som har andre fagområder som ikke nødvendigvis innebærer de overnevnte fagene, informasjonssikkerhet eller personvern. Det pekes og på et aldersskille da yngre har lettere for å forstå og justere sine prosesser enn eldre som har jobbet med det samme og lengre tid og er veldig opptatt hvordan ting har vært i stedet for å se hvordan ting endres eller kan bli bedre.

Informant 14 beskriver en organisering ved anskaffelser som hos dem er viktig for å sikre god bestillerkompetanse:

«En anskaffelse handler om å få delt den inn i 2 områder - det faglige i hva som skal anskaffes med hvilken funksjonalitet må en ha for å løse oppgavene, sett opp mot lovverk, mens IT sin rolle vil være det tekniske og veldig ofte også i forhold til informasjonssikkerhet»

Når en kravspesifikasjon skal utfylles, så må både det faglige i forhold til det leveransen skal tilby defineres, men også forhold rundt cyber-/informasjonssikkerhet, og statens standardavtaler blir trukket frem som et godt verktøy uavhengig om det skal anskaffes under de oppgitte terskelverdiene hvor apparatet ellers ikke er med i prosessen, eller ved større anskaffelser da de tilbyr noe standardtekst rundt personvern og cyber-/informasjonssikkerhet. Det blir i tillegg pekt på nødvendigheten av å ha gode prosedyrer, rutiner og flytprosesser for å sikre at også andre innen andre fagområder kan stille de rette kravene og etterspørre relevant dokumentasjon fra en leverandør.

Samtidig pekes det flere steder på at innkjøp som skjer innen definerte rammer, som eksempelvis en rammeavtale med IT-produkter fungerer veldig bra. Der sikres det god sikkerhet og minimale innkjøp ettersom disse kravene er ivaretatt under anskaffelsen av rammeavtalen og avrop på avtalen skjer vi avtaleeier.

- **Hvordan implementer kommunen/virksomheten cybersikkerhet i anskaffelser?**

Det har vært mye tillit til at leverandørene har god nok sikkerhet og tillit er noe vi nordmenn er flinke på. Som Plikk (2018) beskriver det: «*Vi er et tillitsbasert samfunn».* Men etter flere angrep den senere tiden, så har dette fokuset snudd og det er flere som har begynt å implementere sikkerhet i flere ledd, derav krav i anskaffelser.

«Så min holdning er; når vi skal anskaffe, så må vi ha et sett av krav, de må oppfylles, hvis ikke de oppfylles – «Fuck off», da går vi til neste. Er de oppfylt, da er mye gjort, og da blir det mye enklere med den videre risikovurdering» (Informant 2).

Kravspesifikasjonen som settes med en tverrfaglig gruppe som kommer tidlig inn i anskaffelsen og statens standardavtaler med fokuspunkt på sikkerhet som vi har vært innom før, ble nevnt igjen her av flere informanter. Kommune-CSIRT presiserer at krav til sikkerhet, sammen med en risikovurdering, må tidlig inn for å få en god løsning. Det var flere eksempler på tilfeller hvor dette ikke fungerte, hvor koronapandemien var et ganske dominerende eksempel med begrunnelse i at systemer, produkter og leveranser ble hasteanskaffet for å sikre driften, noe som resulterte i frafall av anskaffelsesrutiner, sikkerhet og risiko.

Foruten det, fant vi noe variasjon når det gjaldt hva slags tiltak de hadde gjort for å implementere cyber- og informasjonssikkerhet i anskaffelsene, men flere informerte om at de hadde, eller var i ferd med å stille krav til at leverandørene skal kunne dokumentere at de oppfyller standarder eller sertifiseringer som NSMs grunnprinsipper for IKT sikkerhet, ISO 27001, ISO 27002, helsenormen og Norsk Helsenett. Men det var spesielt i de store anskaffelsene de hadde fått inn slike krav, og ikke i alle av de mindre anskaffelsene. Det å stille krav om ISO 27001/27002, NSMs grunnprinsipper og lignende til leverandørene er et godt steg, men Orange Cyberdefence poengterer også at en også må ha fokus på hvor leverandørene har opphav, serverplassering og tilstedeværelse, som eksempelvis russisk barnevernsprogramvare som vil være en programvare som innehar høyere risiko for angrep.

Det var også en splittelse i forhold til hvordan case-kommunene opplevde å få leverandørenes dokumentasjon, hvor det stedvis var en utfordring, mens det i andre tilfeller kom automatisk. Men det å kunne ettergå dokumentasjonen fra leverandørene opplevde kommunene litt forskjellig, og i case-kommune 1 og 2 ble det pekt på at dette innad i kommunen ikke blir gjort grunnet manglende kunnskap, mangel på tid eller at det ikke ble prioritert, og spesielt i prosesser hvor det var mange tilbydere opplevde kommune 1 det som problematisk å kunne ettergå all dokumentasjon og etablere et kommunikasjonsforhold med tilbyder for å kunne verifisere hvorvidt de oppfylte kravene eller ikke. I de tilfeller hvor dette ble prioritert og fulgt opp, etterspurte de mer informasjon der dokumentasjonen manglet eller var uforståelig. Kommune-CSIRT sin opplevelse var at det var svært få kommuner som kontrollerte dokumentasjonen i detalj og heller kun aksepterte en referanse til en revisjon.

I flere tilfeller var det en del «vi er i ferd med å...» tiltak som informantene sa de holdt på med å etablere:

- kravdatabase med cybersikkerhetsspørsmål og personvernspørsmål
- universelle krav til leverandøren
- ferdig lagde maler

Selv om dette er gode planer, så er det lite konkret å vise til enda. Men som informant 3 beskrev det:

«det er en liten jobb som gir stor verdi»

Overgangen til skyløsning er fremmet som positivt hos mange, også hos NSM, men Orange Cyberdefence presiserer at skyløsninger også krever en litt annen kompetanse. Dette begrunnes med at skyløsninger har en bedre sikkerhetsløsning, men om en ikke vet hvordan disse innstillingene skal opereres og justeres, så vil sikkerhetsmekanismene i mange tilfeller ikke bli skrudd på og løsningens sikkerhet vil derfor svekkes og miste noe av verdien.

Kommune-CSIRT lister opp 4 lavkost anbefalinger som kommuner kan gjøre for bedre IKT sikkerhet innad leverandørkjeden:

- Flerfaktor autentisering.
- Få administrasjonskontoer og færre rettigheter på brukerkontoer.
- Oppdatert programvare og eliminering av sårbar programvare.
- Segmentering av tilganger og systemer innover i infrastrukturen for å hindre at en aktør som har kommet seg inn kan hoppe videre i infrastrukturen.

- **Hvordan følger virksomheten opp cybersikkerhet hos leverandører under livsløpet og kontraktens levetid?**

SSA avtalene blir igjen henvist til av case-kommune 1 og 2 som et bindende format for hva, hvordan og hvor ofte spesifikke ting skal følges opp, og informant 13 henviste til et bilag som heter «administrative bestemmelser» i alle statens standardavtaler hvor dette dekkes. Ved gjennomgang av flere av statens standardavtaler som kjøpsavtale (SSA-K), avtale om løpende avtalekjøp (SSA-L), standardavtaler for skytjenester (SSA-sky), vedlikeholdsavtalen (SSA-V) og oppdragsavtalen (SSA-O) for å nevne noen, så finner vi riktignok bilagene som referert til, men standardteksten omhandler mye titler og en beskrivelse om hva som kan inngå her som eksempelvis:

«Kunden har rett til å foreta revisjon og verifikasjon av at Leverandøren overholder avtalte forpliktelser for driftstjenesten.» (DFØ, 2019c, s. 15)

Med en presisering i tilhørende avtales bilag 6, administrative bestemmelser:

Kunden skal fastsette eventuelle frister for varsel om revisjon og nærmere prosedyrer for gjennomføring mv., herunder bruk av revisor, her (DFØ, 2018c, s. 14).

Avtalene det refereres til innbyr i liten grad noe som kan binde leverandøren til særskilte sikkerhetskrav for å sikre leverandørkjeden, så kommunene må definere dette på egenhånd. Informanten ga oss innsyn i en av deres avtaletekster hvor den standard avtaleteksten, til dels i hovedavtalen og i stor grad i bilagene, var endret til å være svært spesifikk på hva leverandøren forplikter seg til. Selv om den generelle teksten ikke gir voldsomme krav, så finner vi likevel en tekst i driftsavtalens bilag 6 som spiller relevant inn:

«Leverandørens godkjente underleverandører skal angis her.» (DFØ, 2018c, s.15).

Denne teksten, som står som standard tekst, tilbyr en mulighet for å få kunnskap om full leverandørkjede. Anskaffelsesforskriften (2016, §19-2) viser til maksimalt to i en leverandørkjede, men informant 14 opplever at tredjepartsleverandører blir altfor langt unna virksomheten, og at de har vært nødt til å kreve dokumentasjon om den tredje leverandøren for å ha kontroll på hele kjeden da dette ikke er noe som kommer automatisk.

Men hvor vidt det som er avtalefestet blir fulgt opp under kontraktens levetid var det mye diskusjon rundt. Som vi har sett på tidligere i oppgaven, så er innkjøps-/anskaffelsesenheten et bistandsledd, men eierskapet ligger hos behovshaver og der er det veldig varierende i forhold til hvor mange som følger opp leverandørene.

«Når ting er på plass og ting funker, så slipper du det og løper videre» (Informant 5).

Kommune-CSIRT sin vurdering er at det er noen kommuner som er veldig nøye på dette, men de er i fåtall, og at de aller fleste mangler rutiner for dette.

Et skille mellom små og store leverandører kommer også frem her da store får mer oppfølging og mindre leverandører går i flere tilfelle hele kontraktsperioden ut uten å ha hatt noen krav til revisjon, dokumentasjon eller lignende. IKS virksomhetene ble dratt frem som flinkere på dette området da de har mange avtaler på vegne av kommunene, men også her mener informant 2 at det er en vei å gå for å bli gode nok. Det er og virksomheter som følger leverandørene tett opp, men de opplever at det må etterspørres informasjon hele tiden og

informant 14 viste til en sak hvor de måtte vente månedsvis på en databehandleravtale. Selv om dokumentasjonen må etterspørres, så oppleves det stort sett som uproblematisk og de opplever leverandørene som nøye i dokumentasjonen som blir etterspurt, men at de kan bli flinkere på frister og sikkerhetsdokumentasjon da denne fremgår som noe svak.

Informant 3 trekker frem at det og må skilles på mellom standard krav til dokumentasjon, revisjoner, møtevirksomhet og den slags, og dag-til-dag driftsmessig oppfølging hvor sistnevnte kategori handler om enkelthenvendelser i forbindelse med support eller bistand som eksempelvis en feil i et system eller en plass som må feies. Disse kan flettes inn i hverandre og utløse underliggende krav dersom det er mange hendelser og/eller dårlig oppfølging fra en av partene. Informant 9 og informant 11 trakk også frem hendelsesbasert oppfølging av leverandørene, og da spesielt fokus mot den hendelsen det gjelder, og ikke annen potensiell risiko. Informant 9 trekker frem hvordan de opplever de jevnlige møtene med leverandørene hvor blir det fokus på drift og ikke sikkerhet, og for å sitere informanten informant:

«Der tror jeg ikke at sikkerhetselementet står veldig høyt i fokus, med mindre det har vært hendelser andre steder som har blitt et tema.»

Hendelsesbasert fokus blir også et fenomen som oppstår ved store hendelser, som eksempelvis Østre Toten cyberangrepet hvor hendelsen fikk den fulle oppmerksomhet, men omkringliggende risiko ikke ble nevnt, og selv om denne spesifikke hendelsen ga et godt fokusområde for andre kommuner hvor mange tiltak ble iverksatt for å heve sikkerheten i sine IKT løsninger, så må ikke fokuset på IKT-sikkerhet stoppe der, men følges videre opp (Informant 11).

Men foruten hendelsesbasert fokus, så er kommunene tilbakevendende på temaet tillit til leverandørene, og Kommune-CSIRT opplever at kommunene er slette i etterspørselen av dokumentasjon. Vi ser at det er en todeling ved innhenting av dokumentasjon da noen opplever å få de tilsendt automatisk, mens andre må mase etter den dokumentasjonen de har lagt krav om. Men å kunne verifisere innholdet i dokumentasjonen krever faglig kompetanse, og noen informanter anser behov for tillitt til leverandørene som noe som automatisk fremtvinges ettersom det er vanskelig å verifisere de sikkerhetsløsningene som leverandøren skilter og en må nesten kunne stole på at leverandørene har det de lover på plass. Informant 11 var tydelig i sin mening:

«Det hjelper ikke med lovnader fra leverandørene hvis det skjer en alvorlig hendelse. Da hjelper det ikke å be om beklagelse i etterkant hvis skaden har skjedd og det går ut over innbyggerne».

I enkelte tilfeller kan det være behov for å tillegge sikkerhet i leveransen etter at kontrakten er inngått. Flere av informantene nevnte at leverandørene som oftest er tilbøyelig på dette området, men i mange tilfeller er dette en nokså forhøyet kost enn om dette var med i konkurransen og ved avtaleinngåelsen, og Orange Cyberdefence opplever at kommunene har lave budsjetter på digital sikkerhet, og må gjennom lange og tunge prosesser for å få bevilget penger til ekstra sikkerhetstiltak.

- **Er det spesielle utfordringer med hvordan dagens regelverk for anskaffelser?**

Informantene vurderte anskaffelsesregelverket slik det forelå i dag som ganske godt bygd opp og det foreligger mye tilgjengelig informasjon og veiledninger gjennom åpne kilder og statlige organer, men kanskje veldig detaljert på noen områder og litt mindre andre steder. Foruten det, var det informanter som savnet flere ting som kunne bedret sikkerheten:

«Så, et lite spark tilbake igjen til leverandørene om at de faktisk har en type salgsprosess som er edruelig og gir troverdige og sanne svar, rett og slett» (Informant 5).

Informanten viser til tillit til leverandørene og utfordringer under vektingsprosessen med utfordringene som oppstår når mange leverandører er med i konkurransen ettersom det er svært ressurs- og tidkrevende å ettergå leverandørene på sikkerhetskravene da det handler om mer enn å lese gjennom en dokumentasjon i konkurransen. Det å kunne verifisere at det som blir lovet er hva kommunene ønsker, og sånn det er i dag, så innebærer det å bli bedre kjent med leverandørene, deres infrastruktur, deres løsninger og hvilke sårbarheter og mangler som foreligger, så det blir i stedet vurdert basert på tillit. Frustrasjonen er vel berettiget da informanten ved flere konkurranser har fått dokumentasjon på sikkerhetskrav fra leverandørene, men når kontrakten er skrevet og leveransen er drift satt, så kommer det opp i ettertid at flere ting mangler og da er det veldig ressurskrevende å få gjort noe med det. Tillit blir også trukket frem av informant 9, og som vedkommende sa:

«*...det blir litt som bukken og havresekken.»*

Så ønsket er todelt; å kunne ha noen rettigheter og raske prosesser for å kunne heve en kontrakt og/eller en instans eller et tilsyn som jobber mot slike saker, for det finnes det mange av ifølge informanten.

Et annet problematisk aspekt rundt dagens måte å anskaffe på ligger ikke nødvendigvis i regelverket da det omhandler kost/nytte vurderinger hvor sikkerhet altfor ofte blir vektet lavere og prisen høyere, hvor da prisen innebærer svakere grad av sikkerhet. Men samtidig kan det være noen føringer til sikkerhet som kunne vært med i lovverket ettersom når kommunene la ved sikkerhetskrav i en konkurranse, så var det å anse som et tillegg leverandørene priset høyere og dermed blir konkurransen dyrere for kommunene. Ønsket til informant 12 var derfor klar:

«Et statlig styrt sikkerhetsteam og sikkerhetsregime, så kunne man kanskje ha spart noen penger og fått høyere sikkerhet. Det er min påstand.»

Bakgrunnen er mye lik informant 5 sin begrunnelse; dette er veldig ressurskrevende og igjen blir det pekt på at dette er tid og penger en kommune ikke har for å kunne ettergå slike ting. Derfor er det ønske om at en ekstern part på statlig nivå skal kunne stille de riktige kravene til leverandørene allerede før anskaffelsesprosessen er startet.

Å få krav til sikkerhet inn i lovverket eller andre styrende prosesser som leverandørene må forholde seg til uten at prisen skal skyte i været blir og nevnt av informant 10 med begrunnelse i at krav til sikkerhet er ikke noe alle og enhver som bedriver en anskaffelse besitter og spesielt små kommuner vurderer informanten som svært utsatt ettersom slik kompetanse er mangelvare hos mange. Dette blir svært sårbart når kommunene blir mer og mer digitale fremover. Å få digital sikkerhet inn i lovverket blir fullt støttet av Kommune-CSIRT som presiserer at dette må inn, muligens i form av et rammeverk for digital sikkerhet som kan hjelpe kommunene med denne delen og begrunnelsen var tydelig:

«Du vet norske kommuner er jo sånn at de gjør som de vil med mindre det står noe i en lov eller en forskrift. Og det er jo kanskje derfor det er så mye forskjellige måter å gjøre ting på rundt omkring i kommunene».

Statens standardavtale blir igjen trukket frem som et godt tiltak av hva som ligger tilgjengelig ute og informant 6 benyttet utelukkende disse avtalene som vedkommende forklarte var tilpasset flere ulike formål, men samtidig presiserte informanten at det er tidlig-fase som er nøkkelen i en anskaffelse, det å kunne komme tidlig nok inn med rett kompetanse for å kunne

definere rette sikkerhetsmessige krav. Så informanten så ikke utfordringen med regelverket, men heller det at det skortes på nevnte del, noe vedkommende får støtte i av informant 3 som presiserer at det må foreligge en balanse. Informant 14 hadde en litt annen vri på Statens standardavtaler hvor de ble trukket frem som et godt grunnlag, men med en påstand om at kommune-Norge er for dårlig på å kvalitetssikre det juridiske i avtalene som benyttes, og da spesielt rundt krav til cyber- og informasjonssikkerhet. Informanten anbefalte å ha en jurist til å gå gjennom statens standardavtale med presiseringer i bilag 4, som er tjenestenivå med standardiserte kompensasjoner og få inn en egen tekst på dette (DFØ, 2018b, s. 15).

God tverrfaglig bestillerkompetanse sett opp mot ressurskrevende prosesser for å sikre dette blir trukket frem av flere informanter, og sett opp mot at ressurser er noe kommuner ikke har et veldig overskudd av, så tar det mye tid å sikre alle aspekter, også sikkerhet i en konkurranse. Noen tiltak til sikkerhet har vi referert til over, men utover det er kommunene blanke på hvordan de i tilfelle skulle sikret det noen annen måte.

I forhold til det å stille krav til leverandørene, så poengterte informant 13 at de stilte krav om at leverandørene må kunne dokumentere at de er ISO 27001 kompatible fremfor sertifisert. Bakgrunnen for denne vurderingen var at dette kunne være diskriminerende i forhold til innkjøpsregelverket om de direkte stilte krav til sertifiseringer ettersom dette kan bli ansett som å velge bort leverandører de ikke ville ha. Informanten viste videre til at de opplever at slike krav er nytt i markedet og mange leverandører har ikke mulighet til å levere på dette kravet og da kan falle inn under dette prinsippet. Informant 12 sa følgende om vekting av sikkerhet for valg av en leverandør som er sikrere enn en annen:

> *«Er du sikker nok, så er du kvalifisert. Så sammen med alle kvalifikasjonskrav eller minimumskrav, så blir ikke de vurdert videre ut etter du har tilfredsstilt kravene som er. Og hvis du er sikrere så får du ikke pluss poeng for det».*

Å stille krav til leverandørene vil kanskje også speile hvordan vektingskriteriene blir satt, men flere informanter viser til at de ikke har med noe som vektlegger dette i vurderingsfasen og som virksomhetene må konkurrere om. Dette begrunnes stedvis med at kravene ligger i konkurransen og at en leverandør ikke kan kvalifiseres om de ikke oppfyller kravene. Det er svært krevende å lage en vurderingsbalanse da pris alltid vil være fokus for vekting, og kvalitet nummer to – og dersom sikkerhet hadde blitt med, så hadde det fått en veldig lav prosentandel i den totale vektingen.

6 Drøfting

I denne delen av oppgaven vil vi se på funnene i analysekapittelet og drøfte disse mot teorikapittelet. Med dette som utgangspunkt vil vi forsøke å svare på forskningsspørsmålet; "Hvordan håndterer norske kommuner risikoen for cyberangrep via underleverandørers IKT-tjenester?", samt de andre delspørsmålene vi har skissert.

6.1 Kommunenes kompetansebakgrunn for risiko, risikodefinisjon og metode

Vi ser gjennom våre funn at det gjennomgående benyttes enkle definisjoner og metoder for å jobbe med risiko. Ifølge informantene må det være slik ettersom de som jobber med risiko, både på overordnet nivå og nedover i organisasjonen, mangler faglig tyngde. Basert på våre funn ser vi ingen tung faglig risikoutdanning hos de sentrale ressursene. Flere av informantene hadde mange enkeltfag i andre utdanninger, hvilket er bra, men det gir ikke den gode dybden i risikofaget. Mye av arbeidet nedover i organisasjonene og på overordnet nivå ble basert på veiledere, rådgivning og kjøpte tjenester. Det er positivt at case-kommunene har en tverrfaglig tilnærming til den risikoen som skal vurderes, men som Aven (2015, s. 13) presiserer, så krever det å vurdere risiko også en forståelse for hvilke metoder og modeller som benyttes til hva, hvordan risikoen skal defineres og hvilken kvalitativ informasjon som kan brukes. Kanskje er det tilstrekkelig med veiledere og rådgivning i henhold til metoder, modeller og definisjonsspørsmålet for kommunenes arbeid. Men det avhenger samtidig i større grad av andre myndigheters og samarbeidsaktørers bistand og sistnevnte er, som vi ser i funnene våre, forbundet med en kostnad som er vanskelig for kommunene å ta stilling til når dette er noe som skal måles opp mot mer brukernære tjenester som hjemmetjenester, barnehager, skoler og sykehjem (Informant 5). Kompetanseheving og etterutdanning kan jo være en løsning som vi ser av Jacobsen og Thorsvik (2013, s. 268-269) i teorikapittelet hvor en kan satse på sine medarbeideres utvikling slik at de de blir tryggere i sin rolle, samt beholde kompetente ressurser over tid. Men selv om det er mulig å innhente kompetanse for mer avansert risikoarbeid på overordnet nivå, så vil resten av organisasjonen fremdeles trenge tid og utdanning til å nå ønsket kompetanse/modenhetsnivå. Om vi ser tilbake på Hillson (1997) modell for vurdering av modenhet av organisasjonens evne til å håndtere risiko ville vi plassert kommunene på nivå 2 hvor de jobber avgrenset i organisasjonen med eksperimentell risikohåndtering, og hovedårsaken til det er at de så langt ikke har klart å etablere en definisjon, et system og modell for risiko som hele organisasjonen benytter. I tillegg finner vi at risikokulturen ikke gjennomgående til stede i case-kommunenes organisasjoner, noe som er kriteria for å komme videre opp på Hillsons modenhetskala. Men samtidig samsvarer det

modenhetsnivået vi har vurdert case-kommunene til bra med Jacobsen & Thorsviks (2013, s. 29) beskrivelse av komplekse organisasjoner hvor lav risikokultur er et av kjennetegnene.

I teorikapittelet har vi sett på noen få av veldig mange risikodefinisjoner, -modeller og -metoder, men informant 5 påpekte under intervjuet at det må være en viss form for «pedagogisk tilnærming til dette». Dette har ført til at de har tatt i bruk risikometoder og -modeller av forenklet art for å få flere til å gjennomføre og følge opp risikoer. Mer komplekse modeller har blitt vurdert som for utfordrende for den enkelte ansatte i kommunen å jobbe med, og derfor faller de tilbake på enkle modeller, eller «enkle ROS» som det ble referert til. Men er dette kun på bakgrunn av manglende faglig tyngde? De avanserte modellene er svært tidkrevende og krever innhenting av mye informasjon, stiller krav til diverse utregninger som krever mye ressurser, som igjen medfører tid og kostnader. I tillegg skal dette være en lesbar risikovurdering for flere, og uten forståelse for risikomodellene blir det utfordrende å kommunisere risikoen. Gjennom våre funn ser vi at case-kommunene har forskjellig tilnærming til risiko innad egen organisasjon hvilket kan forbedres gjennom som vi skal komme tilbake til.

NSM (2021b) har vurdert at risikovurderinger i henhold til NS 5832:2014 standarden, eller trefaktormodellen som den heter er foretrukket for å vurdere IKT-risiko, men i de standardmodellene som vi ser blir brukt i de aller fleste tilfeller er sannsynlighet vurdert, noe som går imot standarden og er heller mer i henhold til KiNS modellen, hvor sannsynlighet i matriseoppsettet inngår. I case-kommune 1 kom vi over en risikomal med pre-definert risiko som skulle hjelpe de som ikke hadde dyptgående forståelse innen risikovurderinger, noe som kan ligne personvernkonsekvensvurderinger (DPIA) som er en risikovurdering spesifikk for personvernet. Fordelen med en DPIA, er at den har flere reguleringer i henhold til lovverk, spesielt personvernopplysningsloven (2018) hvor Datatilsynet (u.å.) har definert en rekke kontrollpunkter for vurderingen av personvernkonsekvensene som fungerer som et rammeverk, men som må tilpasses den enkelte virksomhet (Datatilsynet, 2019b, kap. 5). Med et slikt rammeverk gjør det derfor enklere å definere risikoen, hvilket også var meningen i den pre-definerte malen. I figur 3.2 i teorikapittelet illustreres metoden for vurdering av personvernkonsekvenser og har en rekke referansepunkter til personopplysningsloven. Flere informanter trakk frem DPIA som en prosess som ble gjennomført selv om de stedvis innrømmet at det var en svak oppfølging innen dette området også.

Likevel må det skilles mellom overordnet nivå og en IKT-tilnærming, hvor sistnevnte blir nevnt i svært isolerte tilfeller. 3x3, 4x4 og 5x5 matriser lignende KiNS-modellen er nok enklere å følge, samt lesbar for andre da dette etter hvert har blitt en felles forståelse om at det er slik risiko skal vurderes. I tillegg er det vurdert av case-kommunene at disse modellene gir et godt nok nivå av kvalitativ data. Men den felles forståelsen av risikomodeller har også vært under metodisk endring gjennom tidene og modellene som ble benyttet tidligere var langt enklere og tilbydde mindre kvalitativ risikoforståelse, så kanskje det kommer en mer avansert modell om noen år? Det kan derfor fastslås at det er intuitive og enkle modeller som er nøkkelen til å få kommunale virksomheter til å praktisere risikofaget selv om det er ulikheter mellom organisasjonene. Vi ser heller at kommunene praktiserer faget basert på en enkel modell enn at de vegrer seg for arbeidet eller prioriterer det bort på bakgrunn av manglende kompetanse, usikkerhet og mangel på tid.

I risikoarbeidet, spesielt hvor tekniske eller større tiltak skal iverksettes, vil økonomi kunne spille en større rolle og vi finner det interessant at vi fant kjennetegnene til ALARP-prinsippet. ALARP er et risikoprinsipp som ble veldig synlig etter hvert som informantene forklarte prosessene sine gjennom etterstrebelse av lavest mulig risiko og hvordan de måtte gjøre avveininger for å bestemme om ytterligere tiltak for å få ned risikoen skulle/ikke skulle implementeres i form av kost/nytte vurderinger. Selve ALARP prinsippet er ikke nevnt av informantene på navn, men gjenkjennbarheten i denne formen for risikostyring kom tydelig frem. Prinsippet er som nevnt i teorikapittelet bygd på dokumentasjon, hvor identifiserte tiltak skal implementeres, med mindre det kan dokumenteres at det er et urimelig misforhold mellom kostnader/ulemper og nytte. Her kan det oppstå en konflikt med de som er ansvarlige for økonomistyringen, da de vil si nei når risikoen begynner å komme ned på et middels nivå hvor spørsmål mellom kostnad og nyttefunksjon vil oppstå og her brukes det nok mye tid på å få frem hvorfor tiltakene må inn. Dette er ikke alltid like givende når en vet at dette kan gå på bekostning av brukernære tjenester slik som informant 5 beskrev det. Men sett i det store bildet, vil det ikke også være en stor innvirkning på disse tjenestene dersom en kommune opplever et cyberangrep på bakgrunn av at de har neglisjert risikoen eller akseptert en altfor høy risiko? Interessekonflikter om hva pengene skal brukes på mellom sikkerhet og brukernære tjenester må vurderes ut fra hvordan brukernære tjenester vil påvirkes dersom det skortes på sikkerheten, både i det fysiske og digitale. Det er mange områder hvor det skal vurderes risiko og i de tilfellene hvor det er funnet rød risiko, enten cyber eller ei, skal risikoen i henhold til ALARP ha risikoreduserende tiltak. Dessverre ved mange slike tilfeller

vil kostnadene se høye ut og forståelsen er ikke alltid like stor. Gjennom intervjuene med informantene refererer dem til en kamp med mye strev for å få forståelse fra resten av organisasjonen om at god sikkerhet koster.

Funnet av manglende definerte rammer for risikostyring i våre intervjuede case-kommuner kan ha flere årsaker. Den generelle tilbakemeldingen vi fikk fra informantene var at det ofte oppsto tilfeller hvor risikoen ikke ble fulgt opp etter at vurderinger er «ferdigstilt», noen med definerte tiltak som lå på en plan, men ikke fullført, andre med tiltak som delvis var utført og noen uten tiltak i det hele tatt. Dette kan på én side sees i sammenheng med manglende kompetanse og stor usikkerhet som noen medvirkende faktorer, og ulik metodikk innen samme virksomhet og sektor kan være en annen. Et rammeverk for risikostyring kan i mange tilfeller bistå kommunene med god håndtering og mangelen på et implementert rammeverk. Dette kommer vi tilbake til i et eget avsnitt lenger ned i drøftingen

En annen medvirkende årsak til variasjonene vi fant innenfor organisasjonene kan være risikokommunikasjonen, ettersom det kan være utfordrende å formidle hva risikoen faktisk er da risikoene er dynamiske slik som beskrevet i teorikapittelet. Om vi ser på 4 stegs modellen til Aven og Renn (2009), så avhenger det først og fremst av opplæring, så tillit og inkludering for å kunne lykkes med risikokommunikasjon.

Informantene viser til at flere av de ansatte i kommunene ikke anser digital risiko som noe de trenger å bekymre seg for da de har en antakelse om at det er ivaretatt av IKT-avdelingen, uten at de kan referere til hvordan. Her kan man si at silotenkning har kommet til syne innad i kommunene som har deltatt i denne oppgaven. Denne segmenteringen av ansvar og høye graden av spesialisering kan ha ført til at ansvarsfordelingen knyttet til risiko, som i all sannsynlighet har vært vel ment, har ført barriereskapning hvor den enkelte har ulik relevansdefinering. Ved en sterk silotenkning risikerer man å miste kontaktpunkter både horisontalt og vertikalt på tvers av virksomheten samt en manglende fellesforståelse for målsetning (Cilliers & Greyvenstein, 2012).

Risikokommunikasjon trenger ikke å være avgrenset til formidling av definert risiko, men kan benyttes når en organisasjon skal jobbe etter samme risikometodikk og -system. Dette begrunner vi med at de første trinnene er overførbare til risikostyring, da opplæring og kompetanseheving er nøkkelfaktorer for at resten av organisasjonen skal kunne følge og

gjennomføre samme metode og system for risikohåndtering. Samtidig er tillit til metoden og systemet, samt inkludering fra overordnet nivå andre faktorer som vil hjelpe til med en felles metode og strategi for risikohåndteringen. Og som vi finner gjennom datainnhentingen, har ikke case-kommunene kommet forbi dette i sine prosesser. Hovedsakelig er dette på grunn av at de ikke har fastsatt systemet enda, eller at det er i så tidlig fase at de ikke har ikke har allokert ressurser eller klart å koble på resten av organisasjonen enda. Dette er tydelig gjennom flere utsagn som «vi er i ferd med å...», «vi har planer om å..» eller «vi har akkurat...». For en kommune vil en strategi for risikokommunikasjon bidra til at de sprer mer kunnskap ut i alle ledd, noe som også kan ses på som et organisatoriske tiltak. Case-kommunene har implementert tiltak for bevisstgjøring av risiko tidligere for eksempel mot phishing-angrep.

Vi bak denne masteroppgaven spør oss selv: bør det ikke være en felles metode og system å jobbe med uavhengig av kommune? Kommunene er selvstendige, men, vi ser det som hensiktsmessig om det i lov eller forskrift ble definert et sterkere metodesett som kommunene må rette seg etter. Som vi har belyst tidligere i oppgaven stilles det krav til håndtering av risiko i ulike lover, men de sier at det skal håndteres og ikke nødvendigvis hvordan. Frem til det blir definert en beste praksis i lov har kommune-CSIRT påpekt at kommunene vil gjøre som de selv vil og praksis vil sprike mellom dem.

6.2 Kommunenes kompetansebakgrunn for cyber og informasjonssikkerhet

Som nevnt tidligere har vi intervjuet personer som hadde cyber- og/eller informasjonssikkerhet tillagt sin stilling, aller helst som stillingsbeskrivelse med 100% fokus, noe vi fant var veldig variabelt. Det var i stor grad var mindre prosenter avsatt til dette arbeidet, noe informantene selv har reagert på. Informantene med stort engasjement vurderte selv at virksomhetene burde ha minimum en stilling hvor 100% var dedikert til området, og gjerne dedikere arbeidsgrupper til digital sikkerhet over tid med begrunnelse i at dette er et voksende fokusområde gitt kommunenes digitale utvikling. Gjennom intervjuene fant vi ut at cyber- og informasjonssikkerhetsansvarlige jobber tett sammen med databehandleransvarlige, personvernombud og IKT-personell.

Hvor vidt flere av disse funksjonene tilligger samme stilling er uvisst hos de enkelte kommunene, men det er flere viktige funksjoner som jobber mot et felles mål; sikker

ivaretakelse av deres IKT, informasjon og tjenester. Så på et vis foreligger det allerede en arbeidsgruppe som kan ligne en sikkerhetsavdeling, men det er ikke nødvendigvis formalisert.

Vår ekspert hos Orange Cyberdefence var også enig i at stillingene burde rendyrkes og understrekte behovet for å samle disse i fagmiljøer under sikkerhetsavdelinger.

6.3 Kommunenes kompleksitet

Kompleksitet har vi funnet er til stede gjennom teorikapittelets 3.1.8, men samtidig finner vi at teorien til Ihlen (2014, s. 32) om kompleksitet i anskaffelsene også er til stede. Vi skal komme tilbake til sistnevnte, men vi er noe flere informanter anser det å jobbe i en kompleks organisasjon som en utfordring ettersom det er flere utfordringer forbundet med dette. Informant 2 beskriver manglende risikostyring og informant 10 hinter til manglende risikokultur som jo i og for seg beskriver en kompleks organisasjon ifølge Jacobsen og Thorsvik (2013, s. 29), men om vi setter de påstandene i sammenheng med Perrow (1999, s. 78) sin påstand om at kommuner er særlig risikoutsatt, så bør risikostyring i større grad inn i kommunale virksomheter og frustrasjonen til informant 2 og informant 10 blir mer reell.

Perrows syn på tette koplinger sett opp mot Lysnes (2020) beskrivelse av digitale verdikjeder blir i en kommune en stor risiko som må håndteres. At case-kommunene ikke har kommet så langt i arbeidet med risikoorganiseringen og cyber-/informasjonssikkerhet vil medføre en hendelse som venter på å inntreffe raskere om vi skal tenke som Perrow. Det er derfor viktig at kommunene er rustet til å håndtere hendelsene hvor Orange Cyberdefence er bekymret for kommunenes organisering og forventning om at statlige aktører vil være mer aktivt inn i håndtering enn de faktisk vil være.

Cyberangrepet mot Østre Toten er ifølge denne sammensatte teorien en hendelse som en måtte forvente at skulle inntreffe, og det er flere slike hendelser som venter på å inntreffe. De er «normale», men det som blir avgjørende for konsekvensen og sannsynligheten er hvordan kommunene kan detektere mest mulig av nevnte risiko, hvilke tiltak de implementerer, hvordan de følger opp risikoen og hvordan de organiserer egen virksomhet for å kunne håndtere hendelsene. Rapporten om «Risikostyring i digitale verdikjeder» foreslår et rammeverk for risikostyring som bygger på ISO 31000:2018, det samme rammeverket vi har med i dette studie.

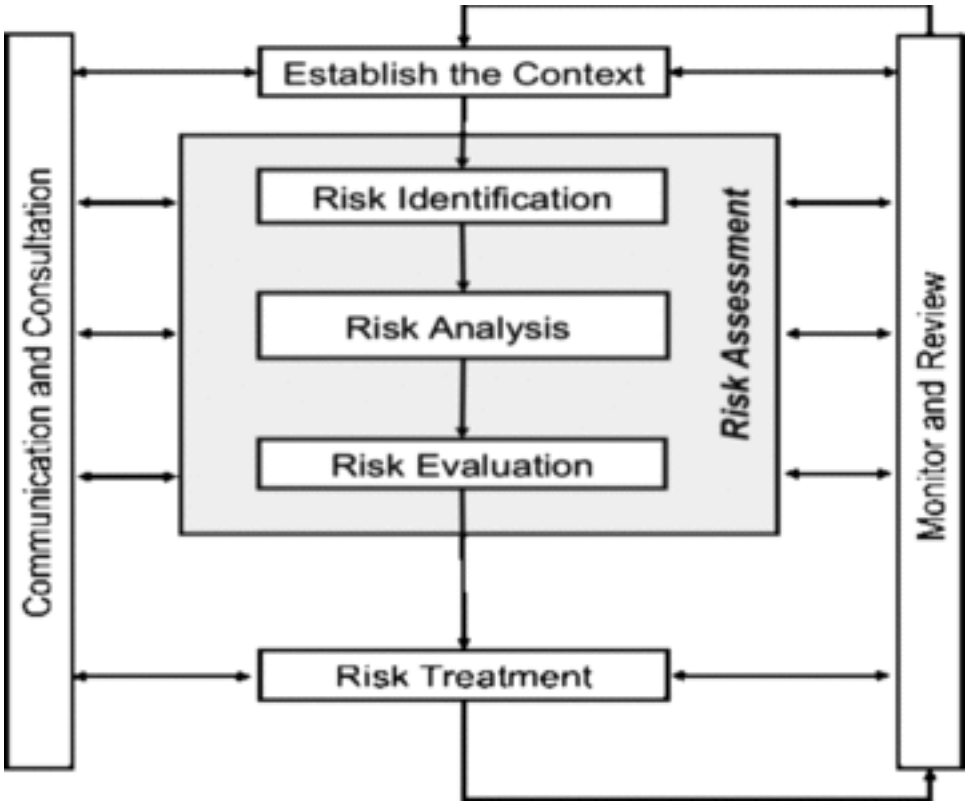
6.4 Rammeverk hos kommunene

Våre funn tyder på at innføring og etterlevelse av standarder og rammeverk for risiko cyber- og informasjonssikkerhet ikke står sentralt innenfor kommunene i denne oppgaven. Standarder var ikke mye utbredt selv om det var mange intensjoner og prosesser som var igangsatt.

I de case-kommunene hvor risikostyringen er knyttet sterkt opp mot internkontrollen, og spesielt KS programmet «Orden i eget hus – Kommunedirektørens internkontroll», ble det forklart som noe som for dem fungerer som et rammeverk for risikostyring. I figur 6.1 vises en modell fra «Orden i eget hus» som sier noe om de forskjellige stadiene. Basert på tilbakemeldingene vi fikk i intervjuene, så var det spesielt den siste rubrikken med «Oppfølging» og sløyfen tilbake i prosessen som var mangelfull i de kommunale virksomhetene.

Figur 6.1 - Modell for risikobasert internkontroll (KS, 2020, s. 65).

Dette modellen kan sammenlignes med prinsippene for risikostyring i henhold til ISO 31000 standarden som ble redegjort for i teorikapittelet og hvor et utdrag av denne modellen vises i figur 6.2. Orden i eget hus fremstår som en forenklet modell i motsetning til ISO 31000 standarden.



Figur 6.2 - Risikostyringsmodell iht. ISO 31000 (Purdy, 2010).

På cyber og informasjonssikkerhet er NSMs grunnprinsipper noe kommunene i størst grad legger til grunn i arbeidet. NSMs grunnprinsipper bygger på ISO 27001/27002, så på mange måter jobber kommunene med mange av de samme tiltakene som vi har dratt frem med ISO-standardene, men på en forenklet måte.

Kommunene kunne med fordel intensivert arbeidet med å ta i bruk standarder og vi i denne oppgaven anbefaler at de på sikt sertifiserer virksomheten innen ISO 27001 da det ville hjulpet med å inkludere avdelingene på tvers og dens ledd nedover. ISO 27000 serien bruker også elementer fra ISO 31000 som igjen er brukt som grunnlaget i "orden i eget hus". Ved å legge 27001 til grunn kan da implementere mye av det som er kjent fra før.

6.5 Kommunenes bruk av Interkommunalt samarbeid

Interkommunalt samarbeid (IKS) ble i denne sammenheng et veldig sentralt tema da flere av case-kommunene hadde organisert seg med dette innen henholdsvis IKT, hendelseshåndtering og anskaffelser. Selv om informanten fra Orange Cyberdefence vurderer interkommunalt samarbeid som en suksessfaktor innad i kommunene, så er tap av intern kompetanse ved utsetting av tjenester en risiko som NSM (2020c) er bekymret for, noe interkommunalt samarbeid innebærer i de tilfellene vi har sett hvor det blir opprettet egne virksomheter uten

lokal tilstedeværelse. Ved utsetting av tjenester vil kommunene få god kompetanse i IKS-virksomheten, men noen kommuner kan tape kompetanse internt og blir veldig avhengige av samarbeidet. En viss intern kompetanse hos eiervirksomhetene er nøkkelen for å kunne ha et effektivt samarbeid, skape en felles forståelse og kunne stille krav til leverandøren da et IKS på mange måter har likhetstrekk med en leverandør ved at de blir betalt (felles kostnadsbilde) mot at de yter tjenester til kommunene.

IKS-virksomhetene har også databehandleravtaler med kommunene hvor de er behandlere av kommunens data. Så intern kompetanse vil her være å anse som bestillerkompetanse ovenfor IKS virksomhetene, og her ser vi stedvis at det blir et gap ved at bestillerkompetansen på vegne av kommunene sitter i IKS-virksomheten, altså har NSM rett i sine bekymringer rundt tjenesteutsetting (2020c).

Men så kan en se på den andre siden av saken ved at dersom kommunen ikke har hatt en slik tjeneste tidligere, men inngår et samarbeid med andre kommuner for tjenesten, vil den da være tjenesteutsatt? Eksemplet vi vil frem til er hendelseshåndteringsteamet (Kommune-CSIRT) da dette er tjenester som er relativt nye for kommunene, og når kommunene så behovet, så ble det etablert et IKS med medlemskostnad. Likevel tilligger ansvaret den enkelte kommunen i henhold til ansvars-, nærhets-, og likhetsprinsippene (Meld. St. 10 (2016-2017), s.20) og ville uansett inngått i kommunens krisehåndteringsorganisering spesifikt mot cyberangrep uavhengig om denne har vært definert tidligere eller ikke. Det kan likevel være trygt å konkludere med at dette er et ansvar som tilligger kommunen og uavhengig av om dette var organisert eller ikke ved inngåelse av en IKS-virksomhet eller kjøp av tjenester fra en slik virksomhet, så er det som Kristiansen (2015, s. 385) beskriver; å tjenesteutsette. Et IKS vil derimot være relevant i henhold til samvirkeprinsippet da dette blir en virksomhet de kan spille på før og etter en hendelse (ikke under) for sikre egen informasjon (Meld. St. 10 (2016-2017), s.20).

6.6 Administrative/organisatoriske/tekniske tiltak og standardisering innad i kommunene

Ulikheter mellom case-kommunene når det gjelder hvordan de jobbet med cyber- og informasjonssikkerhet var definitivt noe som gjenspeilet seg i funnene våre. Vi ser at vi kan skille mellom tre kategorier av tiltak de jobbet med; administrative, organisatoriske og tekniske. Det har kommet noen løft innen cyber- og informasjonssikkerhet de senere år utløst

av angrep enten direkte cyberangrep slik som eksempelvis mot Østre Toten-kommune, eller indirekte årsaker som eksempelvis Russland-Ukraina krigen som gir økte cybertrusler hvor kommunene har fått pålegg fra overordnede myndigheter om å iverksette tiltak. Dette stemmer godt overens med kommentaren fra vår informant fra Kommune-CSIRT om a det i mange tilfeller ikke vil skje noe med mindre det kommer et krav om det i en eller annen form. Og kommentaren fra informant 9 og informant 11 om at utbedringstiltak blir utviklet basert på den konkrete hendelsens art og omfang, men at man ofte neglisjerer andre cyberhendelser som like fullt kan inntreffe. Det er positivt at tiltak iverksettes, men vi mener at tiltakene burde utvikles på grunnlag av definert risiko og sårbarheter, fremfor kun hendelsesbasert utbedring.

Administrative tiltak:

Statens standardavtaler, som våre informanter henviser til ved flere anledninger, er et initiativ fra statlig hold for å bistå offentlige virksomheter med å utarbeide avtaler med leverandørene og krav til sikring av personopplysninger. Som beskrevet i teorikapittelet og i analysekapittelet, er standardene som tilbys i nedlastbar variant fra DFØ sine nettsider veldig lite spesifikke, så å overføre disse direkte, med kun endringer som kunde/leverandør og generelt innhold har liten verdi. Men den avtalen informant 13 viste til var tilpasset kommunene med en rekke nye krav som er spesifikt rettet mot cyber- og informasjonssikkerhet hvilket det da gir en verdi å bruke disse avtalene. Men det krever god tverrfaglig kompetanse å tilpasse avtalene, og når det gjelder cyber- og informasjonssikkerhet, må det foreligge kunnskap om hvilke krav som er relevante for leveransen og på generelt grunnlag, samt hva som kan etterspørres av leverandørene. Om en kommune eksempelvis stiller krav til en sertifisering som ikke er vanlig å finne i norske virksomheter, så vil det utelukke altfor mange aktører. Det vil kunne redusere antall tilbydere, og kanskje resultere i ingen tilbydere i verste tilfelle.

Databehandleravtaler finner vi stort fokus på i våre case-kommuner, men med stort etterslep. Dette er bemerkelsesverdig da krav til databehandleravtaler har eksistert lenge og det ble enda tydeligere med den nye personopplysningsloven (2018, art. 28). Det kan til dels være forståelig med avtaler inngått før 2018, men ikke etter. I offentlige anskaffelser løper avtalene i en tidsbegrenset periode før de igjen må ut på anbud, dvs. nytt avtaleverk, og ettersom det er ganske mange avtaler som reforhandles eller inngås i løpet av ett år, så bør ikke etterslepet være stort. En kunde har også mulighet til å gå tilbake i avtaler der det mangler

databehandleravtale og kreve at dette inkluderes ettersom de er i strid med lovverket. Leverandøren vil også ha interesse av å få en databehandleravtale på plass for å være i henhold til lovverket.

Organisatoriske tiltak

Bevisstgjøring i forbindelse med phishing fant vi at case-kommunene har jevnlige kampanjer på, enten i form av informasjonsformidling alene eller i form av et simulert angrep i tillegg. Men informasjonsformidling blir i samme gate som risikokommunikasjon for øvrig da det etterstrebes å oppnå en felles forståelse av risikoen (phishingangrep), samt hvordan en organisasjon samlet sett kan stå imot slike angrep og da må det benyttes samme tilnærming som vi har sett på tidligere, i form av opplæring, tillit og inkludering. Så om eksempelvis en kommune kjører et simulert phishingangrep uten at organisasjonen vet hva dette er og hvordan de skal håndtere det, så vil det være mange tilfeller hvor ansatte trykker på linker og i verste fall oppgir informasjonen sin ettersom de ikke har forutsetningene for å detektere uønskede e-poster, hvordan håndtere dem og hvem de skal rapportere slikt til. I analysekapittelet ser vi at Orange Cyberdefence og Kommune-CSIRT er forent med at phishing er en høyst relevant angrepsmetode som blir mer og mer avansert slik som NSM (2021a, s 17-20) beskriver i sitt digitale risikobilde. Virksomhetene må da på overordnet nivå sette noen rammer for deteksjon, håndtering og varsling hvorpå de kjører gode bevisstgjøringskampanjer med de ansatte i fremste rekke, noe vi finner at case-kommunene er godt i gang med.

Når det gjelder utvikling av et lagringsregime for hvilken informasjon som skal lagres hvor, så er det gode tiltak dersom de ansatte forstår bakgrunnen for tiltaket og de kan være med på å forbedre cyber- og informasjonssikkerheten i egen virksomhet. Trår en virksomhet feil her vil det ikke hjelpe med sikker lagring da trusselaktørene ved et angrep vil kunne få tilgang på alt som er tilknyttet en bruker, og kommer de seg dypere inn i systemet via en bruker med mange rettigheter, så vil de i verste tilfelle kunne ha tilgang på alt av informasjon som kommunen besitter.

Tekniske tiltak

Vi har tidligere i drøftingen sett på at økonomi og risikoreduserende tiltak står i konflikt og på samme måte finner vi i våre funn at drift og sikkerhet kan komme i konflikt og en god balanse kan være utfordrende å finne. For eksempel, et fagsystem for skolene er noe som må være i drift for at læringsplattformen skal fungere, men slike systemer koster penger og det er, som

nevnt, noe kommunene har et veldig anstrengt forhold til, spesielt ved anskaffelse av systemet. Men når fagsystemet står i fare grunnet manglende sikkerhet, så vil ofte aksjonspunktene omhandle å øke sikkerheten og da muligens også prisen da det må implementeres etter det initiale kjøpet. Dette er et gjennomgående problem som vi får forklart av våre informanter. Og selv om det er noen bedringer enkelte steder, så er det et altfor stort etterslep som vil koste altfor mye penger for å heve graden av sikkerheten.

Vi opplever på bakgrunn av informantenes tilbakemeldinger at case-kommunene ikke har tatt høyde for at sikkerhet må være til stede for å sikre driften og derav er ikke dette med som et vurderingskriteria i anskaffelser. Men vi har sett at hendelser som cyberangrep og cybertrusler som eksempelvis cyberangrepet mot Østre Toten og krigen i Ukraina gir et økt fokus på cyber- og informasjonssikkerhet, både internt og på statlig hold om hendelsen er av større art og interesse. I de tilfeller hvor tiltak blir initiert av statlige myndigheter med krav om at kommunene må ettergå sin digitale sikkerhet, blir det allokert finansielle midler til dette. Det er, som vi har nevnt tidligere, bra for kommunenes sikkerhetsstrategi at det innvilges mer penger, men selv om det blir innvilget mer penger vil det ikke være nok til å dekke alle hull.

Det er også mange eksempler med skygge-IT hvor det mangler god nok sikkerhet og dette er også ukjent risiko for cyber- og informasjonssikkerhetsansvarlige og IKT-personellet. I mange tilfeller ligger det innebygd sikkerhet i IKT-systemene som ikke er aktivert, så at kommunene nå har aktivert disse er enkle tiltak som gir en vesentlig høyere sikkerhet. Disse tiltakene er bra, men kommunene må kunne legge seg på et generelt nivå ved anskaffelser som inkluderer et minimum av sikkerhet som går i balanse med driften. For som vi har sett, så må vi ha sikkerhet for å sikre driften. Likevel har vi funnet tilfeller som motsier dette, og de tilfellene hvor sikkerheten må vike for driften, som vi eksempelvis så under koronapandemien hvor flere virksomheter måtte lette på sikkerheten for å kunne imøtekomme krav om hjemmearbeid under nedstengningsperiodene, så har det vært perioder med omdirigert sikkerhet hvorpå kommunene nå har gjeninnført mer sikkerhet.

6.7 Norske kommuners implementering av cyber og informasjonssikkerhet i anskaffelser

Ihlen (2014, s. 22) viser til at en anskaffelsesprosess skal være tverrfaglig for å få med de gode innspillene og vi ser positivt på at case-kommunenes organisering i forbindelse med en anskaffelse er tverrfaglig, og at samtlige kommuner informerer om at IKT-ressurser (enten fra

IKS eller IKT avdelingen) som minimum skal være med i anskaffelsene for å at gruppen har digital kompetanse. Det overrasker oss derimot at flere av informantene (informant 3, 6, og 13) forteller om at mindre anskaffelser ikke tillegges ressurser og kontroll, noe som betyr at anskaffelsesprosessen ikke får den samme kvaliteten og at kravstillingen til sine leverandører vil kunne bli dårligere. Ihlen (2014, s. 36) viser til forskjellige kompleksitetsnivåer i en anskaffelse og mindre komplekse anskaffelser krever mindre ressurser enn de store og komplekse anskaffelsene. Men likevel må det være grunnleggende krav til leverandører uavhengig kompleksitet ettersom trusselen for leverandørkjedeangrep er tilstede uavhengig av størrelse. Det vil være ulik sannsynlighet for leverandørkjedeangrep med tanke på antall brukere, men konsekvensen vil være lik.

På bakgrunn av at case-kommunene i det minste har et tverrfaglig fokus på de store anskaffelsene kan vi anta at cyberangrep mot disse vil kunne ha en større innvirkning på organisasjonen som helhet og det derfor må sikres i større grad enn de mindre. Likevel må ikke de små anskaffelsene bli glemt da konsekvensen av et leverandørkjedeangrep vil kunne spre seg utover det initiale systemet som blir kompromittert og spre seg gjennom kontaktkjeder i en kommune.

Kravstilling til leverandører

NSMs grunnprinsipper for IKT-sikkerhet (2020b) henviser til at sikkerhet må være en integrert del av prosessene for anskaffelse og utvikling slik at virksomheten minimerer risiko for at nye IKT-produkter og IKT-tjenester innfører konfigurasjonsmessige og arkitekturmessige sårbarheter. Dette sikres gjennom en styringsprosess og godt utformede styringsmekanismer for å kunne kontrollere balansen mellom risiko og drift (Ali & Green, 2009).

Av andre krav vi kan se blir stilt til leverandører, så er det generelle krav til at

«*Dersom Leverandøren engasjerer underleverandør eller Kunden engasjerer tredjepart til å utføre arbeidsoppgaver som følger av denne avtalen, er parten fullt ansvarlig for utførelsen av disse oppgavene på samme måte som om parten selv stod for utførelsen.»* (DFØ, 2020, s. 11).

Likevel foreligger det noen anbefalinger fra sentrale myndigheter som kommunene kan støtte seg på og vi anbefaler at det brukes NSMs 5 viktige anbefalinger for sikkerhet i IKT ved tjenesteutsetting:

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, 2020c, s. 2)

Disse kan med fordel fint overføres til hvilken som helst IKT anskaffelse der en aktør går inn som en leverandør til kommunen, enten i form av direkte leveranse, eller ved hjelp av underleverandører. I tillegg til NSMs grunnprinsipper for IKT-sikkerhet finnes det også andre krav en kommune kan stille til en leverandør, som eksempelvis finnes ISO 27000-serien (Standard Norge, 2018a). Bruken av ISO 27000-serien gir en rekke fordeler, som forutsigbarhet innen IKT-sikkerhet gjennom dokumentasjon, fells terminologi, systematikk og kriterier for resultatoppnåelse (Hoff, 2018).

At en leverandør er ISO 27001-sertifisert eller "compliant" vil ikke nødvendigvis ha stor betydning dersom kommunene selv ikke vet hva det betyr og hvilken dokumentasjon de skal etterspørre for å sikre at leverandøren leverer i tråd med sin egen sertifisering/compliance. Et av våre funn i analysekapittelet var at case-kommunene opplever det som utfordrende å kunne verifisere all informasjon leverandørene leverer, i den grad de leverer den uoppfordret. Case-kommunene har derfor mye tillit til leverandørene når det gjelder hvilke sikkerhetstiltak de har implementert. Hovedårsaken til dette handler om kommunenes interne kompetanse og tid til å ettergå dem.

Dette gjelder også kommunes vurdering om leverandøren etterlever NSMs grunnprinsipper, men disse er mer tilgjengelige for kommunene kontra for eksempel ISO-standardene, da standardene må kjøpes og er en tyngre materie å sette seg inn i. Case-kommunene i denne oppgaven sier at de fokuserer på NSMs grunnprinsipper, med har et langsiktig mål om å bruke ISO 27001-standarden mer aktivt i kravstillingen mot sine leverandører, noe som samsvarer oppfatningen Kommune-CSIRT og Orange Cyberdefence har om kommuner.

Det store aktørene i markedet kan kommunene kanskje stille større krav til, da disse ofte skal ha bedre og mer tilfredsstillende cyber- og informasjonssikkerhet samt dokumentasjon på dette. Det foreligger en differanse mellom store og små/mellomstore virksomheter som vi ser av NSMs vurdering hvor store virksomheter har større verdikjede, større omfang og mer informasjon å beskytte og er bedre rustet gjennom bedre IKT-kompetanse og har i større grad bedre finansiell styrke til å håndtere risikoen for cyberangrep enn mindre virksomheter, og dette er uavhengig om det er i henhold til ISO 27001 eller ei (2020b, s. 12).

Men vi må stille spørsmålet, hvilke krav kan kommunene stille uten at de mister verdifull konkurransekraft og i verste fall står uten en bredde av tilbydere? Ikke alle virksomheter som er tilbydere til kommune-Norge har eksempelvis sertifisert seg eller tatt stilling til "compliance" i henhold til ISO 27001, men har likevel innført tiltak for å bedre sin egen cyber- og informasjonssikkerhet. De tiltakene som er blitt gjort vil høyst sannsynlig kunne krysses av på enkelte kategorier i NSMs grunnprinsipper for IKT-sikkerhet og det kan i større grad være relevant for kommunene å stille krav til dette rammeverket fremfor en ISO-standard for informasjonssikkerhet da krav om ISO-sertifisering kan bety at veldige adekvate leverandører må stå over konkurransen selv om produktene/tjenestene deres treffer bra på kravene for øvrig og vil kunne tilføre kommunene stor verdi.

Men om det ikke stilles krav til en spesifikk modell, sertifisering eller et rammeverk for cyber- og informasjonssikkerhet som kan ettergås på begge sider av bordet, så vil det kunne foreligge en uklar oppfatning av hvilket sikkerhetsnivå leverandørene skal legge seg og sin tjeneste på. Om en kommune stiller målbare krav om at leverandøren skal være i henhold til for eksempel NSMs grunnprinsipper for IKT-sikkerhet eller ISO 27001, så vil det kunne være referansepunkter som begge parter kan avsjekke. Dog stiller dette igjen krav til kommunene da det er primært de som må utarbeide sjekkpunktene som de skal verifisere opp mot leverandør.

<u>Kommunenes bestillerkompetanse</u>
NSM (2018c) fremhever og en bekymring om at sikkerhet ikke er med i anskaffelser og case-kommunene peker selv på at de på generell basis kunne ha sikret bedre bestillerkompetanse innen cyber-/informasjonssikkerhet, men at det ikke gjøres kan igjen begrunnes med mangel på ressurser og stor avstand mellom de som skal gjennomføre anskaffelsen og de som sitter på denne kompetansen.

NSM (2020c) er tydelige på at sikkerhetskompetansen bør være med i anskaffelsene og ikke i form av standard krav da de må kunne stille riktige krav på bakgrunn av en vurdert risiko, men vår oppfatning er at bestillerkompetanse muligens likevel kan sikres midlertidig på andre måter som gjør at ressursene ikke trenger å delta like aktivt i hver eneste anskaffelse, men heller kunne formidle en rekke standard krav som skal være med i enhver anskaffelse, liten som stor.

Likevel ønsker vi å presiseres at risiko og kravstilling til leverandørene ikke må komme for sent inn da den er vanskelig å reforhandle. Som beskrevet i teorikapittelet, presiserer Mehti (2016) at påvirkningskraften for anskaffelsene er i første fase hvor det skal avklares behov og konkurransen skal planlegges, noe vi og ser i figur 5.1 som er henvist til i analysekapittelet. Uten standardiserte krav, god nok bestillerkompetanse og god tverrfaglig fagkompetanse i denne fasen er det større sannsynlighet for at virksomheter med cyber- og informasjonssikkerheten får tilslag på konkurransen og over tid kunne utsette kommunen for potensielt økt risiko.

Utvelgelse av leverandør basert på sikkerhet

Våre funn tilsier at informantene mener det ikke foreligger noen direkte utfordringer med anskaffelsesregelverket slik det foreligger i dag, men samtidig dukker det opp noen utfordringer og ønske om forbedring.

En utfordring som dukker opp er i vektingskriteriene ettersom disse i hovedsak settes til blant annet pris og kvalitet, utenom at det foreligger kriterier i henhold til sikkerhet. Kanskje er det ikke relevant å måle tilbydere på punktet om sikkerhet i sluttfasen, men da er det kritisk at det er kravstilt tidligere i anskaffelsesprosessen og brukt til å vurdere om de er kvalifisert.

Sitatet til Kommune-CSIRT om at kommunene i prinsipp gjør som de vil dersom det ikke er nedfelt i lov er interessant å knytte opp mot informant 10 og 12 sitt ønske om å få mer krav til digital sikkerhet inn i lovverket slik det er gjort med andre ting. Dette vil heve sikkerhetsnivået i mange anskaffelser, spesielt de over som har er verdi på over 100 000,- slik som beskrevet i teorikapittelet.

Informant 13 sitt poeng om diskriminering ved utvelgelse, eller som det generelle likebehandlingsprinsippet i veileder til anskaffelsesforskriften beskriver; *«det skal sikre at*

alle potensielle leverandører gis like muligheter» (Nærings- og fiskeridepartementet, 2018, s. 59-60), har et poeng i henhold til dagens sikkerhetsbilde ved at leverandørene ikke kan stilles for strenge krav slik vi så på tidligere i drøftingen. Likevel ser vi i våre funn at dette bildet er i ferd med å endre seg og at strengere krav over tid kan implementeres. Sitatet til informant 12 om at en leverandør må kvalifiseres til å være sikker nok vil derfor måtte tilpasses markedet og utvikles over tid.

Oppfølging av leverandører

At det også her er funnet variabler mellom oppfølgingen av store og små kontrakter anses å være sårbart da endringer i små kontrakter kan være inngangsvektoren til et stort angrep som vi har nevnt tidligere i drøftingen. En kontrakt skal følges opp og mye kan formaliseres i en avtale, men én ting er å inngå en avtale om revisjoner, møter, verifiseringer og justeringer av både cyber- og informasjonssikkerhet og leverandørens underleverandører som benyttes i forbindelse med kontrakten, men en annen ting er å faktisk etterleve disse og det skal komme på initiativ fra begge parter. Det er litt variable funn i forhold til oppfølgingen i case-kommunene og mens informant 5 viser til at de ikke har tid til å følge opp leverandørene og leverandørkjeden, så er utfordringen til informant 14 det at det er mer utfordrende å følge opp underleverandørene. I teorikapittelet viser vi til Karlsens (2018, s. 214) rutiner for å håndtere en kontrakt hvor det er viktig med bred oppfølging gjennom faste møter hvor alt av avtalens bestemmelser gjennomgås for å se om det fremdeles er gjeldende og justere i henhold til behov, også nedover i leverandørkjeden.

Kommune-CSIRT presierer at sikkerhet i alle ledd er viktig for å unngå angrep, noe flere av våre informanter også nevner og at det er viktig å inkludere leverandørene i dette arbeidet. Informantene opplevde at cyber- og informasjonssikkerhet fikk altfor lite fokus og for lite ressurser på begge sider av leverandørkjeden, noe som gjør oppfølgingen begrenset.

Når det kun blir oppfølging etter hendelser blir det lett for at det kun er fokus på den aktuelle hendelsen slik informant 9 og informant 11 henviste til, og ikke den brede oppfølgingen som beskrevet i teorikapittelet. At sikkerheten ofte uteblir i disse oppfølgingsmøtene er sårbart, men når hendelsen ikke kan isoleres og går utover innbyggerne, så er det alvorlig (Informant 11). Den generelle oppfølgingen som avtales mellom partene er tross alt et forebyggende arbeid mot hendelser og derfor er det viktig å ha tett dialog og jevnlige møter, samt innfri på de punktene begge partene er enige om, selv om det er veldig lett å slippe avtalen og la drift

være drift som informant 5 beskriver, men man ønsker samtidig ikke en ny hendelse slik som i Østre Toten-kommune. Og sikkerhet må tross alt være til stede for å sikre drift (Kommune-CSIRT).

Informant 10 trakk også frem skjult risiko hos leverandører i form av endringer som ikke blir kommunisert, eller at informasjonen ikke kom frem til rette vedkommende. Det ble pekt på at eiere av avtalen ikke videreformidler eller ikke forstår hvordan endringen vil påvirke risikoen, og derfor lar være å formidle videre. I andre tilfeller er det leverandørene som gjør endringer uten å informere videre. Dette kan være sårbarheter i et system som kommunen har kjøpt eller et system som leverandøren benytter med en sårbarhet som kan være en inngang for angrep i en leverandørkjede og som er et eksempel på faktorer som virksomhetene ikke har tatt med i sine vurderinger.

Vi anbefaler kommunene å legge opp en strategi for leverandøroppfølging etter ISO 27001 A.15 slik at avtalt nivå for tjenesteleveranse, cyber og informasjonssikkerhet avsjekkes og eventuelt reforhandles i etterkant av anskaffelsen basert på endring i risiko/trusselbildet.

Reforhandling av sikkerhet

Det koster å kravstille i ettertid og som vi finner i analysekapittelet. Case-kommunene påpeker at det ikke er det å kravstille leverandørene under en driftsfase som er en utfordring, men kostnadene og dersom dette gjelder mange leverandørkjeder, så multipliseres de opp. I de tilfellene hvor kontrakt er inngått uten spesielle krav til leverandørenes IKT-tjenester og det avdekkes at det foreligger en risiko for angrep via dem, kan kommunene kreve høyere grad av sikkerhet. Men så lenge kravene ikke annet er definert under anskaffelsen, vil det bety at leverandørene kan prise sine endringer mot kommunene og her er gjerne ekstrakostnaden større enn om dette hadde vært med fra starten. Dette er kostnader som det ikke er rom for i budsjettene og vi ser at det ikke umiddelbart foreligger penger til å kunne styrke kravene til sikkerhet med alle leverandørkjedene, hvilket vil være et reelt behov gitt stort etterslep ifølge kommunene selv. Alle parter er nok tjent med at slike krav til leverandørers cyber- og informasjonssikkerhet kommer inn i anskaffelsens første fase slik Mehti (2016) presiserer og NSM (2018c) anbefaler.

6.8 Opplevelse av skygge anskaffelser og IKT

Ved flere tilfeller har alle case-kommunene opplevd at det anskaffes digitale løsninger uten at relevante ressurser innen cyber- og informasjonssikkerhet er involvert i prosessen. Dette er et reelt problem hvor det er prosesser uten kontroll som fører til stor potensiell sårbarhet og risiko. Vi har tidligere pekt på varierende kompetanse innen dette området, mangel på tid og tvetydig ansvar som vil være medvirkende faktorer for den helhetlige kontrollen av anskaffelser.

Som gjengitt i teorikapittelet er det ulike terskelverdier i offentlige anskaffelser hvor det stilles få krav til styring og kontroll når totalsummen er under kr. 100 000,- (Vigander, 2022) som gjør anskaffelse av skygge IT enklere gjennom direkteanskaffelse (Nærings- og fiskeridepartementet, 2018, s. 45). Som vi ser i case-kommune 1 i denne oppgaven, blir ikke disse direkteanskaffelsene underlagt anskaffelsesenheten, hvilket betyr at krav, styring og kontroll uteblir og i disse tilfellene ender det ofte som skygge-IT som bærer med seg risikofaktorer man ikke får tatt høyde for.
Vår anbefaling til kommunene er å kjøre skanninger på sine nettverk for å identifisere eventuell forekomst av skygge IT på nettverket. Dette kan ses på som en del av asset managment i ISO 27001 hvor det handler om å ha oversikt over egen infrastruktur (Standard Norge, 2017b, s. 11).

Ved funn står virksomheten over flere valg, og det første er å inkorporere det anskaffede systemet i porteføljen til kommunen, men dette krever i noen tilfeller et ekstra innlegg av sikkerhet om løsningen ikke allerede har det rette nivået. Alternativt må de forkaste systemet, og i våre funn ser vi flere tilfeller i case-kommunene hvor det har blitt anskaffet systemer og IKT utstyr hvor dette ikke lar seg implementere i deres oppsett som da medførte at de måtte stoppe prosessen og ta det ut av infrastrukturen (Informant 5; Informant 11; Informant 14). I slike tilfeller vil ofte kontrakten ha en form for oppsigelsestid, eventuelt en kontraktsperiode som uansett må løpe med gjeldende kostnader. Et siste alternativ kommunene har er å integrere systemet slik det står og akseptere risikoen dette innebærer.

6.9 Kommuners opplevelse av myndighetenes arbeid med risiko, cyber- og informasjonssikkerhet

Myndighetene, slik de er definert i analysekapittelet, er både statlige og kommunale virksomheter som har i oppgave å bistå blant annet kommuner. Er de samkjørt nok for kommunenes beste?

Som vi ser i innledningen og analysekapittelet, er det mange aktører som skal jobbe mot kommunene på dette området og det er lett for at det blir rot om kommunikasjonen og samarbeidet dem imellom ikke fungerer tilstrekkelig. Hver aktør skal finne beste praksis som de anser som anvendelig, og som de kommuniserer ut til sine målgrupper, som i denne sammenheng er kommunene. Utfordringen dreier seg ikke alene om denne aktøren, men når neste aktør gjør det samme bare med en annen metode som de anser som beste praksis, så kan det bli rot ettersom det da dukker opp problemstillinger når det gjelder hvem kommunene skal forholde seg til. Når det også dukker opp eksempelvis 5 andre aktører som har samme mål og målgruppe, så blir det enda mer komplisert.

Dette står i stil med og kan ses på som silotenkning eller sektortenkning (Cilliers & Greyvenstein, 2012) fra myndighetenes side. Slik det er i dag har myndighetene sterke vertikale skiller ved at departement styrer egne sektorer og blir i den grad "siloer" eller beholdere med informasjon. Silotenkningen og ansvarsfordelingen har ført til at alle har utviklet sine egne veiledere, fra eget perspektiv og at de føler at de er best til å vite fra sitt ståsted. Uten at vi har snakket med myndighetene selv er det en fare for at det opereres med en "oss/dem" mentalitet mellom sektorer hvor systematisk og helhetlig tenkning uteblir (ibid).

Samtlige av informantene etterlyser en samkjøring av en metode som er universelt tilpasset kommunene i Norge, men å finne en beste praksis-metodikk som passer alle kommunene vil være utfordrende. Det kan kanskje være en tanke å kutte antall aktører som skal jobbe med kommunene og heller la de få gjenværende inngå et samarbeid slik at antall metoder og beste praksiser blir minimert.
Basert på dagens organisering og kompetansenivå er det spesielt to myndighetsinitiativer case-kommunene mener er velfungerende:

- NSMs grunnprinsipper for IKT-sikkerhet blir vurdert som et godt fungerende sett med prinsipper for cybersikkerhet som case-kommunene finner intuitivt og lettere å jobbe etter fremfor standardene ISO 27001 og ISO 27002.

- KS sin versjon av «Orden i eget» hus blir trukket frem som en fungerende veileder for implementering og styring av risiko på overordnet nivå, men det gjenstår noe arbeid med å få modellen og metoden benyttet i hele organisasjonen med en felles forståelse for hvilken risiko som finnes og hvorfor det ligger en verdi i å håndtere dem i fellesskap.

Det finnes mange metoder og modeller for vurdering av risiko, men våre resultater viser at kommunene må ha det forenklet da de som risikoorganisasjoner ikke er modne for de mer avanserte modellene per dags dato.

Når det gjelder hendelseshåndtering ved oppståtte cyberangrep viser resultatene at noen av informantene har en forventning om at eksempelvis Nasjonalt cybersikkerhetssenter (NCSC) eller politiet skal bistå dem, men som Orange Cyberdefence påpekte er det sjeldent disse tilbyr bistand utover varsling og generell rådgivning ved inntrufne hendelser. Informant 12 sa følgende:

«Et statlig styrt sikkerhetsteam og sikkerhetsregime, så kunne man kanskje ha spart noen penger og fått høyere sikkerhet. Det er min påstand.»

Enkelte kommuner har innsett dette og informanter har informert at de har inngått avtaler med andre aktører på det private markedet som eksempelvis Orange Cyberdefence for å dekke opp for det. Ifølge Kommune-CSIRT er hendelseshåndtering noe kommunene per nå bør organisere internt fremfor å kjøpe denne tjenesten via eksterne leverandører. Kommunene kan eksempelvis bygge dette inn i eksisterende beredskaps- og kriseorganisasjon, men det må foreligge en form for kunnskap om hvordan en skal kunne håndtere slike cyberangrep spesifikt. Det er gjort en del erfaringer fra tidligere hendelser, erfaringer som har endt opp i læringspunkter som kan kommuniseres og tiltak som kan anbefales, men når det ikke foreligger noen krav, ei heller noen oppfølging foruten informasjon og anbefalinger, så vil det ikke føre til like slagkraftig utbedring på cyber- og informasjonssikkerhet i kommunene. Det står kanskje ikke på viljen, men penger og kompetanse er noe som fortsatt blir vurdert som mangelvare i kommunene. Informant 2 påpeker at det foreligger risiko for at et vedkommende uten faglig kunnskap og forståelse ender opp i sikkerhetsroller uten at de vet hva det innebærer

7 Konklusjon

På ulike måter har informantene i denne studien hjulpet å besvare vårt forskningsspørsmål «Hvordan håndterer norske kommuner risikoen for cyberangrep via leverandørenes IKT-tjenester?» og underspørsmålene: «Hvordan implementerer norske kommuner risiko og cybersikkerhet i anskaffelser?» og «Hvordan opplever norske kommuner myndighetenes arbeid med risiko, cyber- og informasjonssikkerhet?».

Tilbakemeldingene fra informantene var gode og at dette er et veldig viktig tema. De håper at med sin deltagelse setter risiko, cyber- og informasjonssikkerhet i leverandørkjedene høyere på agendaen i norske kommuner. Ene informanten vår sa "*Smi mens jernet er varmt"* med klar referanse til cyberangrepet mot Østre Toten.

Under vil vi prøve å oppsummere kort:

«Hvordan håndterer norske kommuner risikoen for cyberangrep via leverandørenes IKT-tjenester?»

Våre resultater i denne oppgaven viser at case-kommunenes organisering innehar flere interkommunale samarbeidsvirksomheter, hvor spesielt IKT peker seg ut. Det er ingen faglig tung risikokompetanse og det benyttes kompetanseheving og kjøpte tjenester i risikoarbeidet. Kompetanse innen cyber- og informasjonssikkerhet finner vi å være til dels god.

Case-kommunene er til dels beviste på risikoen for cyberangrep mot leverandørkjedene og jobber med å få økt sin kontroll. Det er en lav modenhetsgrad når det gjelder risiko, men basert på langsiktige planer er det tydelig at kommunene er i ferd med å implementere, eller at det forelå planer om å implementere system, felles definisjon av risiko, felles metodikk og felles forståelse av arbeidet. Endringer tar tid og dette er en kultur som skal snus hvilket er utfordrende i en organisasjon, og spesielt i komplekse organisasjoner som har vi funnet at kommunene er.

Risikomodellene for gjennomføring av risikostyring er enkle og det benyttes en simpel definisjon av risiko som sannsynlighet x konsekvens = risiko. Etter vår vurdering passer dette kommunene per dags dato da kommunene ikke er modne for mer avanserte modeller. Kriterier for risikoaksept finner vi ikke definert, men at den blir håndtert ulikt i de forskjellige prosessene fra gang til gang. Kommunene kan med fordel bruke trefaktormodellen for risiko etter anbefaling fra NSM og definert risikoakseptkriterier etter ALARP prinsippet etter hvert som virksomheten blir mer moden med fagkunnskap.

Videre kan de med fordel jobbe med å inkludere hele organisasjonen gjennom å etablere et rammeverk for risikostyring og informasjonssikkerhet inkludert en strategi for risikokommunikasjon. I sum vil dette være med å motvirke silotenkning og "oss/dem" mentalitet innad i kommunene.

«Hvordan implementerer norske kommuner risiko og cybersikkerhet i anskaffelser?»

I de større anskaffelsene ser det ut til å være lagt opp gode prosesser med tverrfaglig deltagelse inkludert roller innen cyber- og informasjonssikkerhet, personvernombud og IKT-personell som sikrer bestillerkompetanse basert på en tydelig tolkning av anskaffelsesregelverket, men i de mindre anskaffelsene blir dette tillagt mindre fokus, noe som gjør at disse ikke får samme kvalitet og at direkteanskaffelser utenfor prosesser kan finne sted og inngå i virksomhetens skygge IT. Vi ser fremdeles at prosessene ikke alltid følges da ressursene tidvis kommer sent inn i anskaffelsen, noe som er problematisk med tanke på påvirkningskraften som faller over tid.

Sikkerhet som vektingskriterium under tilbudskonkurranser anses å ikke være relevant da dette i utgangspunktet bør ivaretas gjennom kravstillelse og kvalifikasjonsvurdering i anbudsprosessen. Om det skulle vært vurdert implementert bør det være vesentlig forskjell mellom sikkerhetsnivået til de ulike tilbyderne.

Videre kan kommunene med fordel integrere et bedre sett med standard krav til cyber- og informasjonssikkerhet i sine anskaffelser. Det er viktig å påpeke at disse må ettergås av personer med fagkompetanse under vurdering og utvelgelse samt at de også må kunne måles i leverandøroppfølgingen over tid. Vi foreslår at kommunene fortsetter å bruke NSM grunnprinsipper, men at de også med fordel kan vurdere å bruke ISO 27001 "compliance" mer utstrakt i kravstillingen mot sine leverandører. Skillet mellom sertifisert og "compliant" er viktig for å ikke havne i fellen hvor de ekskluderer gode tilbydere som er viktige å ha med for å få bredde i konkurransen.

« Hvordan opplever norske kommuner myndighetenes arbeid med risiko, cyber- og informasjonssikkerhet?»

Det er mange aktører på myndighetsnivået som jobber mot kommunene med formål om å styrke deres kompetanse til å kunne håndtere risiko for cyberangrep, enten det er gjennom veiledning til metoder, modeller, definisjoner, standarder og rammeverk. Per dags dato viser det seg å stedvis være for mange, som i forlengelse benytter ulike tilnærminger og praksiser

slik at det blir uoversiktlig og overveldende for de kommunale virksomhetene å forholde seg til. Dette har ført til at vi tør å påstå at silotenkning har vokst frem på tvers av sektorene i offentlig sektor. For å motvirke denne tenkningen kan man med fordel minimere antallet myndighetsaktører som bidrar på cyber- og informasjonssikkerhetsområdet mot norske kommuner, hvor de gjenværende bør settes i et mer koordinert samarbeid hvor for eksempel Nasjonalt cybersikkerhetssenter eller NSM sentralt får en koordinerende rolle.

Det kan med fordel ryddes blant de tilgjengelige veilederne slik at en mer samlet tilnærming kommer til syne. Det vil være ryddigst om det standardiseres én felles risikomodell/-metode som kan dekke norske kommuners behov. Modellen som presenteres av KiNS med en 5x5 matrise i form av sannsynlighet x konsekvens vurderes å være passende for kommunene per i dag gitt ulikt kompetansenivå innad kommunene, samt et felles mål om å bli en risikostyrt organisasjon. På sikt anbefaler vi som sagt å legge NSMs trefaktormodellen til grunn etter hvert som kunnskapsnivået til kommunene øker.

Kommunene i denne oppgaven etterlyser generelt en statlig virksomhet med faglig tyngde som kan bistå dem ved eventuelle cyberangrep. Det foreligger aktører som arbeider med varsling, for eksempel kommune CSIRT, men det er begrenset hvilken nytte en kommune kan dra av disse om det ikke foreligger en videre bistand tilknyttet deteksjonsvarselet dersom virksomheten opplever et angrep. En etablering av et hendelseshåndteringsteam (IRT) på statlig nivå som rykker og ut bistår kommunene i en hendelse kunne vært med å heve beredskapen betraktelig. Inntil en slik løsning er på plass, vil kommunene være best tjent med å inkludere denne kompetansen i egen eksisterende beredskaps- og kriseorganisasjon, eller å kjøpe tjenestene på det kommersielle markedet.

8 Videre forskning

I denne oppgaven har vi innhentet data fra 3 kommuner i mellomstor størrelsesorden (25 000 – 35 000 innbyggere) for å se hvordan de jobber med risiko for leverandørkjedeangrep, deres implementering av cybersikkerhet i anskaffelser og deres opplevelse av myndighetenes arbeid innen risiko og cybersikkerhet. Under datainnhentingen ble det referert til at det vil være annerledes i mindre og større kommuner hvilket kan være interessant å se hvordan det samme oppleves i disse perspektivene. Eller om en kan se dette fra et større kommunalt bilde hvor flere deltagende kommuner deltar med en differensiering mellom mindre, mellomstore og store kommuner gjennom en kvantitativ datainnhenting.

Referanser

Abdullah, L. M. & Verner, J. M. (2012). Analysis and application of an outsourcing risk framework. *The Journal of Systems and Software, 85*(8), 1930–1952. https://doi.org/10.1016/j.jss.2012.02.040

Al-Safwani, N., Fazea, Y., & Ibrahim, H. (2018). ISCP: In-depth model for selecting critical security controls. *Computers & Security, 77*, 565–577. https://doi.org/10.1016/j.cose.2018.05.009

Ali, S. & Green, P. (2009). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers*, *14*(2), 179–193. https://doi.org/10.1007/s10796-009-9183-y

Anskaffelser. (2022, 15. februar). *Anskaffelsesprosessen steg for steg.* https://anskaffelser.no/anskaffelsesprosessen/anskaffelsesprosessen-steg-steg

Anskaffelsesforskriften (2016) *Forskrift om offentlige anskaffelser.* (FOR-2016-08-12-974). Lovdata. https://lovdata.no/dokument/LTI/forskrift/2016-08-12-974

Anskaffelsesloven. (2016). *Lov om offentlige anskaffelser* (LOV-2016-06-17-73). Lovdata. https://lovdata.no/dokument/NL/lov/2016-06-17-73?q=lov%20om%20offentlige%20anskaffelser

Aven, T. (2015). *Risk Analysis.* 2. utg. Wiley.

Aven, T. (2020). *The Science of Risk Analysis. Foundation and Practice.* Routledge.

Aven, T. & Renn, O. (2009). The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk. *Risk Analysis*, *29*(4), 587–600. https://doi.org/10.1111/j.1539-6924.2008.01175.x

Bachlechner, D., Thalmann, S. & Maier, R. (2013). Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective. *Computers & Security*, Vol 40, s. 38-59. https://doi.org/10.1016/j.cose.2013.11.002

Barne- og likestillingsdepartementet. (2009). *Etiske krav i offtentlige anskaffelser.* Regjeringen. https://www.regjeringen.no/globalassets/upload/bld/for/ie_veileder_for_etisk_handel.pdf

Bernard, A. (2022, 7. Juni). Humans still weakest link in cybersecurity. *The republic.* https://www-techrepublic-com.cdn.ampproject.org/c/s/www.techrepublic.com/article/humans-weakest-link-cybersecurity/amp/

Busmundrud, O., Maal, M., Kiran, J.H. & Endregard, M. (2015). *Tilnærminger til risikovurderinger for tilsiktede uønskede handlinger* (FFI-rapport 2015/00923). Forsvarets forskningsinstitutt. https://publications.ffi.no/nb/item/asset/dspace:2503/15-00923.pdf

Center for Internet Security (CIS) (u.å.). *The 18 CIS Critical Security Controls.* Hentet 18. Juni 2022 fra https://www.cisecurity.org/controls/cis-controls-list

Cilliers, F. & Greyvenstein, H. (2012). The impact of silo mentality on team identity: An organisational case study. *SA Journal of Industrial Psychology, 38*(2), e1–e9. https://doi.org/10.4102/sajip.v38i2.993

Cox. (2008). What's Wrong with Risk Matrices? *Risk Analysis*, *28*(2), 497–512. https://doi.org/10.1111/j.1539-6924.2008.01030.x

Cox, R. (2014). *Risk Assessment and Planning for Offshore Oil Spill Response Preparedness*. http://dx.doi.org/10.2118/168336-MS

Damanpour, F., Magelssen, C., & Walker, R. M. (2020). Outsourcing and insourcing of organizational activities: the role of outsourcing process mechanisms. *Public Management Review*, *22*(6), 767–790. https://doi.org/10.1080/14719037.2019.1601243

Datatilsynet. (u.å.). *Sjekkliste for vurdering av personvernkonsekver (DPIA).* Hentet 25. juni 2022 fra https://www.datatilsynet.no/globalassets/global/dokumenter-pdfer-skjema-ol/regelverk/veiledere/dpia-veileder/sjekkliste-for-dpiafaser.pdf

Datatilsynet. (2018a, 23. juni). *Skytjenester.* https://www.datatilsynet.no/personvern-pa-ulike-omrader/internett-og-apper/skytjenester/

Datatilsynet. (2018b, 30. Oktober) *Iverksette styringssystem for informasjonssikkerhet.* https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

Datatilsynet. (2019a, 17. juli.) *Hva er personvern.* https://www.datatilsynet.no/rettigheter-og-plikter/hva-er-personvern/

Datatilsynet. (2019b, 17. juli). *Vurdering av personvernkonsekvenser (DPIA).* https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Dhillon, G., Syed, R., & Sá-Soares, F. de. (2017). Information security concerns in IT outsourcing: Identifying (in) congruence between clients and vendors. *Information & Management, 54*(4), 452–464. https://doi.org/10.1016/j.im.2016.10.002

Digdir. (u.å.) *Hva er håndtering av risiko?* Hentet 5. juli 2022 fra https://www.digdir.no/informasjonssikkerhet/hva-er-handtering-av-risiko/3041

Digi. (2021, 24. Februar). *Microsoft: Over 1000 hackere sto bak Solarwinds-angrepet.* https://www.digi.no/artikler/microsoft-over-1-000-hackere-sto-bak-solarwinds-angrepet/507205

Digitaliseringsdirektoratet (Diri). (u.å.). *The story.* Hentet 18. Juni 2022 fra https://diri.ai/story/

Dimitri, N., Piga, G. & Spagnolo, G. (2011) *Handbook of procurement.* Cambridge University Press.

Direktoratet for e-helse. (2020a, 4. februar). *Normen – Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren.* https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren#1.6%20Normens%20utvikling%20og%20forvaltning

Direktoratet for e-helse. (2020b, 5. februar). *Vedlegg – Samlet oversikt over normens krav.* https://www.ehelse.no/normen/normen-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren/Vedlegg%20Oversikt%20over%20Normens%20krav.docx

Direktoratet for forvaltning og økonomistyring. (u.å.) *Anskaffelsesprosessen steg for steg.* DFØ. Hentet 22. mai 2022 fra: https://anskaffelser.no/anskaffelsesprosessen/anskaffelsesprosessen-steg-steg

Direktoratet for forvaltning og økonomistyring. (2018a). *SSA-L bilag 2018 (bokmål).* DFØ. *https://anskaffelser.no/sites/default/files/2021-11/ssa-l_bilag_2018.docx.docx*

Direktoratet for forvaltning og økonomistyring. (2018b). *SSA-D bilag 2018 (bokmål) (docx).* DFØ. https://anskaffelser.no/sites/default/files/ssa-d_bilag_2018_bok.docx

Direktoratet for forvaltning og økonomistyring. (2019a). *SSA-O generell avtaletekst 2018 (bokmål) (docx).* DFØ. https://anskaffelser.no/sites/default/files/ssa-o_generell_avtaletekst_2018_bok.docx

Direktoratet for forvaltning og økonomistyring. (2019b). *SSA-S generell avtaletekst 2018 (bokmål) (docx).* DFØ. https://anskaffelser.no/sites/default/files/ssa-s_generell_avtaletekst_2018_bok.docx

Direktoratet for forvaltning og økonomistyring. (2019c). *SSA-D generell avtaletekst 2018 (bokmål) (docx).* DFØ. https://anskaffelser.no/sites/default/files/ssa-d_generell_avtaletekst_2018_bok.docx

Direktoratet for forvaltning og økonomistyring. (2020). *SSA-K generell avtaletekst 2018 (bokmål) (docx).* DFØ. https://anskaffelser.no/sites/default/files/ssa-k_generell_avtaletekst_2018-bok.docx

Direktoratet for forvaltning og økonomistyring. (2021a, 8. november). *Divisjon for offentlige anskaffelser.* DFØ. https://anskaffelser.no/dfos-arbeid-med-offentlige-anskaffelser/divisjon-offentlige-anskaffelser

Direktoratet for forvaltning og økonomistyring. (2021b). *SSA-sky generell avtaletekst versjon 2021.* DFØ. https://anskaffelser.no/sites/default/files/2022-05/ssa-sky_generell_avtaletekst_v2021.docx

Direktoratet for Samfunnssikkerhet og Beredskap. (2016) *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* DSB. https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Dvergsdal, H. & Nätt, T.H. (2019, 2. desember). Sårbarhet (IT). I *Store norske leksikon.* *https://snl.no/s%C3%A5rbarhet_-_IT*

Engen, O. A, Kruke , I. K, Lindøe, P.H, Olsen, O.E og Pettersen, K.A (2016). Perspektiver på samfunnsikkerhet. Cappelen damm akademisk. Oslo.

Europol, European Cybercrime Centre (2019, 9. oktober) *INTERNET ORGANIZED CRIME THREAT ASSESSMENT (IOCTA)*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2019#downloads

Fan, Z.-P., Suo, W.-L., & Feng, B. (2012). Identifying risk factors of IT outsourcing using interdependent information: An extended DEMATEL method. *Expert Systems with Applications*, *39*(3), 3832–3840. https://doi.org/10.1016/j.eswa.2011.09.092

Feng, & Li, M. (2011). An information systems security risk assessment model under uncertain environment. *Applied Soft Computing*, *11*(7), 4332–4340. https://doi.org/10.1016/j.asoc.2010.06.005

Foreningen for kommunal informasjonssikkerhet (KiNS). (u.å.). *Mal for gjennomføring av risikovurdering.* Hentet 28. juni 2022 fra https://kins.no/verktoykasse/mal-for-gjennomforing-av-risikovurdering/

Frost, C. (2000). Outsourcing or increasing risks? *Emerald Insight*, Vol. 8(2), s. 34-37 https://doi.org/10.1108/09657960010338599

Gottschalk, P. (2005a). *Outsourcingledelse.* Oslo: Cappelen Akademiske forlag.

Gottschalk, P. (2005b). *Sourcing av IT-tjenester. Lokalisering, organisering og styring av ITfunksjoner*. Kristiansand: Høyskoleforlaget

Grenlandssamarbeidet. (u.å.). *Anskaffelsesreglement Bamble-, Drangedal-, Kragerø-, Porsgrunn-, Siljan- og Skien kommune.* Hentet 24. april 2022 fra https://www.grenlandssamarbeidet.no/contentassets/1ce5165c97904fbca76713b566f4a566/gki/drift/2019/vedtatt-nytt-anskaffelsesreglement-for-grenlandskommunene-.pdf.pdf

Hafting, T. (2017) *Krisehåndtering – planlegging og handling.* Fagbokforlaget.

Harstad kommune. (u.å.). *Anskaffelsesreglement for Harstad kommune.* Hentet 24. april 2022 fra https://harstad.kommune.no/eknet/docs/pub/DOK00754.pdf

Helgestad, B. (2022, 16. april). *Angrepet på Østre Toten kommune.* Telenor. https://www.telenor.no/om/digital-sikkerhet/2021/angrep-pa-ostretoten.jsp

Helse- og omsorgtjenesteloven. (2011). *Lov om kommunale helse- og omsorgstjenester m.m.* (LOV-2011-06-24-30). Lovdata. https://lovdata.no/dokument/NL/lov/2011-06-24-30

Hillson, D. A. (1997). Towards a risk maturity model. *The international journal of project & Business risk management*, *1*(1), 35-45. https://risk-doctor.com/wp-content/uploads/2020/06/RMM-IJPBRM-Mar97.pdf

Hoff, B. (2018, 4. april). Standarder for IKT-sikkerhet – verktøy eller sovepute? NSM. https://nsm.no/hold-deg-oppdatert/meninger/standarder-for-ikt-sikkerhet-verktoy-eller-sovepute

Hol kommune. (u.å.). *Anskaffelsesreglement for Hol kommune.* Hentet 24. april 2022 fra https://www.hol.kommune.no/siteassets/hol/dokumenter/teknisk-eiendom-og-naring/naring/anskaffelser/anskaffelsesreglement-hol-kommune-2020.pdf

Hutchins, E., Cloppert, M. & Amin, R. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. *Leading Issues in Information Warfare & Security Research* (1). https://www.researchgate.net/publication/266038451_Intelligence-Driven_Computer_Network_Defense_Informed_by_Analysis_of_Adversary_Campaigns_and_Intrusion_Kill_Chains

Ihlen, G.B. (2014) Anskaffelsesprosessen: En praktisk tilnærming til forberedelse og gjennomføring. Universitetsforlaget. Oslo.

IKS-loven. (1999). *Lov om interkommunale selskaper.* (LOV-1999-01-29-6). Lovdata. https://lovdata.no/dokument/NL/lov/1999-01-29-6

International organization for standardization (2018a). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. (ISO/IEC 27000:2018) ISO/IEC 27000:2018(en), Information technology — Security techniques — Information security management systems — Overview and vocabulary

International organization for standardization (2018b). *Risk management – Guidelines*. (ISO 31000:2018en). https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Jacobsen, D-I. & Thorsvik, J. (2013). *Hvordan organisasjoner fungerer* (4. utg.). Fagbokforlaget

Johannesen, A., Tufte, P.A. & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskapelig metode* (5. utg.). Abstrakt forlag.

Jones, C (2021) Warnings (& lessons) of the 2013 target data breach. *Red River.* https://redriver.com/security/target-data-breach

Karlsen, J. T. (2018). *Prosjektledelse – fra initiering til gevinstrealisering* (4. utg.). Universitetsforlaget

Kaurel, F-E. (2020, 11. Oktober). Leverandør. I *Store norske leksikon.* *https://snl.no/leverand%C3%B8r*

Khalfan, A. M. (2004). Information security considerations in IS/IT outsourcing projects: a descriptive case study of two sectors. *International Journal of Information Management*, *24*(1), 29–42. https://doi.org/10.1016/j.ijinfomgt.2003.12.001

Knudsen, E. (2021, 28. juni) Microsoft – hackerne har nå angrepet Microsofts egen kundestøtte. *Digi.no*. https://www.digi.no/artikler/solarwinds-hackerne-har-na-angrepet-microsofts-egen-kundestotte/511541

Kobezak, P., Machandy, R., Raymond, D. & Tront, J. (2018). *Host Inventory Controls and Systems Survey: Evaluating the CIS Critical Security Control One in Higher Education Networks.* University of Hawai'i. http://hdl.handle.net/10125/50486

Koc, T. & Bozdag, E. (2017). Measuring the degree of novelty of innovation based on Porter's value chain approach. *European Journal of Operational Research*, *257*(2), 559–567. https://doi.org/10.1016/j.ejor.2016.07.049

König, A. & Spinler, S. (2016). The effect of logistics outsourcing on the supply chain vulnerability of shippers Development of a conceptual risk management framework. *The International Journal of Logistics Management*, *27*(1), 122–141. https://doi.org/10.1108/IJLM-03-2014-0043

Kommunal- og distriktsdepartementet. (2016, 18. april). *Nasjonal strategi for bruk av skytjenester.* Regjeringen. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-bruk-av-skytenester/id2484403/

Kommunal- og distriktsdepartementet. (2022, 9. mars). *Sikkerhetstiltak i norske kommuner i forbindelse med Russlands invasjon av Ukraina.* Regjeringen. https://www.regjeringen.no/contentassets/f2a8e2c722644a6ea153395c0b15dc05/sikkerhetstiltak-i-norske-kommuner-i-forbindelse-med-russlands-invasjon-av-ukraina.pdf

Kommuneloven. (2018). *Lov om kommuner og fylkeskommuner* (LOV-2018-06-22-83). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-22-83

Kristiansen, H. (2015) Utkontraktering fra finansforetak. *Lov og rett*, *7*, 383–402. https://doi-org.ezproxy.uis.no/10.18261/ISSN1504-3061-2015-07-02

KPMG (2021, 26. august). *IKT-sikkerhet i Østre Toten kommune forut for dataangrepet 9. januar 2021 – kartlegging og ekstern vurdering.* https://www.ototen.no/_f/p1/i5689ceb7-72b4-44d0-970c-a5c4828047e5/endelig-rapport-26082021-kpmg_sladdet.pdf

Langø, H-I. & Sandvik, K. B. (2013a). Cyberspace og sikkerhet. *Internasjonal politikk, 71*(2), 221–228. https://doi.org/10.18261/ISSN1891-1757-2013-02-05

Lee, C.K.M., Yeung, C., & Hong, Z. (2012). An integrated framework for outsourcing risk management. *Industrial Management + Data Systems*, Vol. 112(4), s. 541–558. https://doi.org/10.1108/02635571211225477

Lupton, D. (2013). *Risk* (2. utg.). Routledge

Lysne, O. (2020). *Risikostyring i digitale verdikjeder.* (Rapport 2422). Direktoratet for samfunnssikkerhet og beredskap (DSB). https://www.dsb.no/rapporter-og-evalueringer/risikostyring-i-digitale-verdikjeder/

Mahieu, K. (2001). Vertikale avtaler i IKT-sektoren. Om bakgrunnen for gruppeunntaket for vertikale avtaler og anvendelsen av det innen informasjons- og kommunikasjonsteknologi. *Tidsskrift for forretningsjus*, *7*(1), 62–133. https://doi.org/10.18261/ISSN0809-9510-2001-01-05

Mandiant. (2020, 13. Desember). *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor.* https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

Marelli, M. (2022). The SolarWinds hack: Lessons for international humanitarian organizations. *International Review of the Red Cross (2005)*. https://doi.org/10.1017/S1816383122000194

Maal, M., Krogedal, K. & Gjengstø, A. (2020). *IKT-sikkerhet i anskaffelser og tjenesteutsetting i kraftbransjen – sjekkliste* (NVE rapport 1/2020). Norges vassdrags- og energidirektorat. http://publikasjoner.nve.no/rapport/2020/rapport2020_01.pdf

Mark, M.S., Tømte, C. E., Næss, T., & Røsdal, T. (2019). Leaving the windows open – økt mangel på IKT-sikkerhetskompetanse i Norge. *Norsk Sosiologisk Tidsskrift*, *3*(3), 173–190. https://doi.org/10.18261/issn.2535-2512-2019-03-02

Markussen. (2017). Mindre konkurranse om offentlige anskaffelser? *Stat & styring*, *3*, 38–41. https://doi-org.ezproxy.uis.no/10.18261/ISSN0809-750X-2017-03-12

Meld. St. 10 (2016-2017). *Risiko i et trygt samfunn – Samfunnssikkerhet.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/meld.-st.-10-20162017/id2523238/?ch=8

Methi, M. (2016). *Samfunnsansvar ved innkjøp i norsk kommuner - bare en følelse? : en studie av hvordan fire norske kommuner implementerer samfunnsansvar ved anskaffelser*. Universitetet i Agder ; University of Agder. http://hdl.handle.net/11250/2433977

Microsoft Exchange team. (2021, 2. mars) *March 2021 Exchange Server Security Updates*. https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

Midtun, B. (2022, 22. mars). 12 ting du må vite om cyberangrep og cybersikkerhet. *Sintef.* https://www.sintef.no/siste-nytt/2021/12-ting-du-ma-du-vite-om-cyberangrep-og-cybersikkerhet/

Nasjonal Sikkerhetsmyndighet. (2015). *Helhetlig IKT-risikobilde 2015.* NSM temarapport. https://nsm.no/getfile.php/133681-1592831865/Filer/Dokumenter/Rapporter/nsm_helhetlig_ikt_risikobilde_2015_lr.pdf

Nasjonal Sikkerhetsmyndighet (2018a) *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting – En utdyping av området «Beslutt leveransemodell» i NSMs grunnprinsipper for IKT sikkerhet.* NSM temarapport. https://nsm.no/getfile.php/133447-1591950720/Filer/Dokumenter/Rapporter/Temarapport%20Landvurdering%20tjenesteutsetting.pdf

Nasjonal Sikkerhetsmyndighet (2018b) *Hva bør du tenke på hvis du skal tjenesteutsette?* NSM temarapport. https://nsm.no/aktuelt/hva-bor-du-tenke-pa-hvis-du-skal-tjenesteutsette

Nasjonal Sikkerhetsmyndighet. (2020a, 14. Desember). *Oppdatert informasjon om SolarWinds Orion.* NSM varsler. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/oppdatert-informasjon-til-solarwinds-orion

Nasjonal Sikkerhetsmyndighet. (2020b, 15. april). *NSMs grunnprinsipper for IKT-sikkerhet. Versjon 2.0.* NSM veileder. https://nsm.no/getfile.php/133735-1592917067/Filer/Dokumenter/Veiledere/nsms-grunnprinsipper-for-ikt-sikkerhet-v2.0.pdf

Nasjonal Sikkerhetsmyndighet. (2020c, 1. juli). *Sikkerhetsfaglige anbefalinger ved tjenesteutsetting.* NSM veileder. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/sikkerhetsfaglige-anbefalinger-ved-tjenesteutsetting/

Nasjonal Sikkerhetsmyndighet. (2020d, 12. august). *Ofte stilte spørsmål om sky og tjenesteutsetting.* NSM veileder. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/ofte-stilte-sporsmal-om-sky-og-tjenesteutsetting/sky-tjenesteutsetting-og-sikkerhet/

Nasjonal Sikkerhetsmyndighet. (2020e, 26. august) *Grunnprinsipper for IKT-sikkerhet*. NSM veileder. https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt

Nasjonal Sikkerhetsmyndighet. (2021a, 28. Oktober). *Nasjonalt digitalt risikobilde 2021*. NSM rapport. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/nasjonalt-digitalt-risikobilde-2021

Nasjonal Sikkerhetsmyndighet. (2021b). *Risikovurdering av IKT-systemer.* NSM rapport. https://nsm.no/getfile.php/136603-1625054089/Filer/Bildegalleri/Bilder%20til%20grunnprinsipper/Risikovurdering%20av%20IKT-systemer.pdf

Nasjonal Sikkerhetsmyndighet. (2021c, 11. mars). *Risiko 2021 – helhetlig sikring mot sammensatte trusler.* NSM rapport. https://nsm.no/aktuelt/risiko-2021-helhetlig-sikring-mot-sammensatte-trusler

Nasjonal Sikkerhetsmyndighet. (2022a, 25. Mars). *Åpen kildekode i den digitale leverandørkjeden.* NSM. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/nyheter-fra-ncsc/apen-kildekode-i-den-digitale-leverandorkjeden

Nasjonal Sikkerhetsmyndighet. (2022b, 11. februar). *Risiko 2022. Økt risiko krever økt årvåkenhet.* NSM. https://nsm.no/getfile.php/137798-1644424185/Filer/Dokumenter/Rapporter/NSM_rapport_final_online_enekeltsider.pdf

Nasjonal Sikkerhetsmyndighet. (2022c, 24. februar). *Oppdatert situasjonsbilde fra NCSC.* NSM rapport. https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/oppdatert-situasjonsbilde-fra-ncsc

Nicho, M. (2018). A process model for implementing information systems security governance. *Information and Computer Security*, *26*(1), 10–38. https://doi.org/10.1108/ICS-07-2016-0061

Njå, O., Sommer, M., Rake, E.L. og Braut, G.S (2020) *Samfunnssikkerhet. Analyse, styring og evaluering.* Universitetsforlaget

Norsk Helsenett. (u.å.a) *Risikostyring.* Hentet 18. juni 2022 fra https://www.nhn.no/om-oss/Personvern-og-informasjonssikkerhet/sikkerhetsarbeid-internt-i-norsk-helsenett/risikostyring

Norsk Helsenett. (u.å.b) *Om oss.* Hentet 18. juni 2022 fra https://www.nhn.no/om-oss

Norsk Hydro. (2020, 14. Oktober). *Cyberangrep på Hydro.* https://www.hydro.com/no-NO/media/pa-dagsorden/cyberangrep-pa-hydro/

Norsk Senter for informasjonssikring. (2020, 27. februar). *Trusler og Trender 2019-2020: Verdikjedeangrep en av de største digitale truslene mot norske virksomheter.* NorsSIS https://norsis.no/ny-rapport-verdikjedeangrep-en-av-de-storste-digitale-truslene-mot-norske-virksomheter/

Norsk Senter for informasjonssikring. (2021a, 15. mars). *NSMs risikorapport 2021: Koronapandemien har forsterket det eksisterende risikobildet.* NorSIS. https://norsis.no/nsms-risikorapport-2021-koronapandemien-har-forsterket-det-eksisterende-risikobildet/

Norsk Senter for informasjonssikring. (2021b, 24. Mars). *Trusler og trender 2021.* NorSIS. https://norsis.no/content/uploads/2022/05/NorSIS_Trusler_Trender_2021_Digital.pdf

NOU 2006:6. (2006). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske samfunnsfunksjoner.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2006-6/id157408/

NOU 2015:13. (2015). *Digital sårbarhet – sikkert samfunn — Beskytte enkeltmennesker og samfunn i en digitalisert verden.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/

NOU 2018:17. (2018). *Klimarisiko og norsk økonomi.* Finansdepartementet. https://www.regjeringen.no/no/dokumenter/nou-2018-17/id2622043/?ch=1

NSM, PST & Etterretningstjenesten. (2010). *Bakgrunnsnotat Cybersikkerhet* (2010/00719/430 utg.). Forsvarsdepartementet. https://www.regjeringen.no/contentassets/252f869fdfac46648e41e6ca5fb0600a/cybersikkerhet_svar-med-merknader_nsm-pst-etterretningstjenesten.pdf

Nærings- og fiskeridepartementet. (2018, 24. April). *Veileder til reglene om offentlige anskaffelser (anskaffelsesforskriften).* Regjeringen. https://www.regjeringen.no/no/dokumenter/veileder-offentlige-anskaffelser/id2581234/

Nærings- og fiskeridepartementet. (2017, 30. mai). *Nytt anskaffelsesregelverk.* Regjeringen. https://www.regjeringen.no/no/tema/naringsliv/konkurransepolitikk/offentlige-anskaffelser-/forste-kolonne/nytt-anskaffelsesregelverk/id2518659/

Orange Cyberdefence. (2021, 28. mars). *SolarWinds sends a message: it is time to be proactive about security.* https://www.orange-business.com/en/magazine/solarwinds-sends-message-it-time-be-proactive-about-security

Os kommune. (2017). *Anskaffelsesreglement (offentlige anskaffelser) for Os kommune.* https://os.kommune.no/wp-content/uploads/2020/10/Reglement-for-anskaffelser-Os-kommune.pdf

Oslo kommune. (u.å.). *Oslomodellen.* Hentet 24. april 2022 fra https://www.oslo.kommune.no/for-vare-leverandorer/krav-til-leverandorer/oslomodellen/#gref

Perlekar, N. & Thakkar, J. J. (2019). Risk management framework for outsourcing in the defence sector: a case from India. *International Journal of Production Research*, *57*(18), 5892–5919. https://doi.org/10.1080/00207543.2018.1555381

Perrow, C. (1999). *Normal Accidents. Living with High-Risk Technologies.* Princeton University Press.

Personopplysningsloven. (2018) *Lov om behandling av personopplysninger.* (LOV-2018-06-15-38). Lovdata. https://lovdata.no/dokument/LTI/lov/2018-06-15-38

Pettersen, L. (2018). Digitalisering. *Norsk medietidsskrift*, *25*(4), 1–17. https://doi.org/10.18261/ISSN.0805-9535-2018-04-03

Plikk, N. (2018, 26. september). Nordmenn er rike, godtroende og naive. *TEK.NO.* https://www.tek.no/nyheter/nyhet/i/EWm08K/nordmenn-er-rike-godtroende-og-naive

Politiets sikkerhetstjeneste. (2022) *Nasjonal trusselvurdering 2022.* PST. https://www.pst.no/alle-artikler/trusselvurderinger/ntv-2022/

Prado, E.P.V. (2011). Risk analysis in information technology and communication outsourcing. *Journal of Information Systems and Technology Management*, Vol. 8(3), s. 605-618. https://doi.org/10.4301/S1807-17752011000300005

Prop. 1 S (2016-2017). *For budsjettåret 2017.* Justis- og beredskapsdepartementet. https://www.regjeringen.no/no/dokumenter/prop.-1-s-jd-20162017/id2513950/?ch=1

Purdy, G. (2010). ISO 31000:2009-Setting a New Standard for Risk Management. *Risk Analysis*, *30*(6), 881–886. https://doi.org/10.1111/j.1539-6924.2010.01442.x

Renn. O. (2008). *Risk Governance. Coping with Uncertainity in a Complex World.* Earthscan from Routledge.

Renn, O., Walker, K. D., & International Risk Governance Council. (2008). *Global Risk Governance : Concept and Practice Using the IRGC Framework* (1st ed. 2008., Vol. 1). Springer Netherlands : Imprint: Springer.

Samsvar. (u.å.) *I samsvar med alle regler på en og samme plattform.* Hentet 18. juni 2022 fra https://www.samsvar.net/

Sarpsborg kommune. (2017). *Anskaffelsereglement for Sarpsborg kommune.* https://www.sarpsborg.com/globalassets/anskaffelsesreglement---vedtatt.pdf

Schartum, D. W. (2021). Jus og digitalisering. *Lov og rett,* 60(2), 92–109. https://doi.org/10.18261/issn.1504-3061-2021-02-04

Seim, T.W. (2002). Konkurranseutsetting - offentlige -anskaffelser og anbud. Feil i saksbehandlingen og erstatningsansvar. *Tidsskrift for Forretningsjus, 8*(2), 175–181. https://doi.org/10.18261/ISSN0809-9510-2002-02-03

Shala, D. (2021, 17. juni). *Etterforskningen av datanettverksoperasjonen mot statsforvalterembeter henlegges.* PST. https://www.pst.no/alle-artikler/pressemeldinger/etterforskningen-av-datanettverksoperasjonen-mot-fylkesmannsembetene-er-avsluttet/

Sikkerhetsloven. (2018). *Lov om nasjonal sikkerhet.* (LOV-2018-06-01-24). Lovdata. https://lovdata.no/dokument/NL/lov/2018-06-01-24

Sirnes, E. & Stoltz, G. (2017, 2. oktober) Kostnad-nytte analyse. I *Store norske leksikon.* https://snl.no/kostnad-nytte-analyse

Sivilbeskyttelsesloven. (2010). *Lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret.* (LOV-2010-06-25-45). Lovdata. https://lovdata.no/dokument/LTI/lov/2010-06-25-45

Standard Norge (2017a) *Informasjonsteknologi Sikringsteknikker Ledelsessystemer for informasjonssikkerhet Krav* (ISO/IEC 27001:2013 innbefattet Cor 1:2014 og Cor 2:2015). https://www.standard.no/en/PDF/FileDownload/?redir=true&filetype=Pdf&preview=true&item=913029&category=5

Standard Norge (2017b). *Informasjonsteknologi Sikringsteknikker Ledelsessystemer for informasjonssikkerhet Krav* (ISO/IEC 27001:2013 innbefattet Cor 1:2014 og Cor 2:2015).

Standard Norge (2017c). *Informasjonsteknologi Sikringsteknikker Tiltak for informasjonssikring* (ISO/IEC 27002:2013 innbefattet Cor1:204 og Cor 2:2015*).*

Standard Norge (2018.) *Informasjonsteknologi - Sikringsteknikker - Risikostyring for informasjonssikkerhet.* (NS-ISO/IEC 27005:2018).

Standard Norge. (2022, 11. mars). *Grunnpakke 1-2-3 for cybersikkerhet.* (NS-ISO 27000). https://www.standard.no/fagomrader/ikt/it-sikkerhet/grunnpakke-1-2-3-for-cybersikkerhet/

Startoff. (u.å.) *Digital overvåking av kritisk infrastruktur.* Hentet 5. juli 2022 fra: https://startoff.anskaffelser.no/digital-overvaking-av-kritisk-infrastruktur

Statistisk sentralbyrå, *IKT-strategier (prosent), etter status for strategi, forvaltningsnivå, statistikkvariabel og år. 2021-2022.* [Online]. Hentet fra: https://www.ssb.no/statbank/table/12019/tableViewLayout1/

Statistisk sentralbyrå, *Offentlig forvaltning. Lønnskostnader, vare- og tjenestekjøp og investeringer, etter sektor og formål (mill. kr) 2007 – 2021.* [Online]. Hentet fra: https://www.ssb.no/statbank/table/10726

Sultana, N. & Tamanna, M. (2021). Exploring the benefits and challenges of Internet of Things (IoT) during Covid-19: a case study of Bangladesh. *Discover Internet of Things*, *1*(1), 1–12. https://doi.org/10.1007/s43926-021-00020-9

Sundlisæter, T. (2013, 23. april). Forbereder Norge på cyberangrep. *Teknisk ukeblad*. https://www.tu.no/artikler/forbereder-norge-pa-cyberangrep/234825

Symantec. (2019, Februar) *ISTR – Internet Security Threat Report* (Vol. 24). https://docs.broadcom.com/doc/istr-24-2019-en

Telenor. (u.å.) *Hva er cyberangrep?* Hentet 4. juli 2022 fra https://www.telenor.no/sikkerhet/cyberangrep/

Telenor. (2021). *Digital Sikkerhet 2021.* https://www.telenor.no/om/digital-sikkerhet/2021.jsp

Thurén, T. (2015) *Vitenskapsteori for nybegynnere* (2. utg.) Oslo: Gyldendal Akademisk

Uldal, L.S. (2013) *Pasientmotivasjon for gastric bypass : en kvalitativ studie*. [Masteroppgave]. Norwegian University of Life Sciences, Ås. http://hdl.handle.net/11250/188419

Van der Haar, H. & von Solms, R. (2003). A model for deriving information security control attribute profiles. *Computers & Security*, *22*(3), 233–244. https://doi.org/10.1016/S0167-4048(03)00311-0

Vigander, K. (2022, 22. April). *Nye EØS-terskelverdier for 2022-2024.* KS. https://www.ks.no/ks-advokatene/nyheter/nye-eos-terskelverdier-for-2022-2024/

Vinnem, J-E. & Røed, W. (2020). *Offshore Risk Assessment Vol. 1. Principles, Modelling and Applications of QRA Studies.* 4th edition. Springer.

Visma. (2019, 6. Februar). *Intelligence report recognises Visma's contribution to illuminate threats and protect organisations from cyberespionage.* https://newsroom.visma.com/pressreleases/intelligence-report-recognises-vismas-contribution-to-illuminate-threats-and-protect-organisations-from-cyberespionage-3121558

Wangen, G. B. (2017) *Cyber Security Risk Assessment Practices: Core Unified Risk Framework*. NTNU. http://hdl.handle.net/11250/2447264

Weiner, R. (2018) *Hacker linked to Target data breach gets 14 years in prison*. The Washington post. https://www.washingtonpost.com/local/public-safety/hacker-linked-to-target-data-breach-gets-14-years-in-prison/2018/09/21/839fd6b0-bd17-11e8-b7d2-0773aa1e33da_story.html

Weltzien, K. & Lande, H. (2008). Når anskaffelsen haster.
Nærmere om «umulighetsterskelen» over og under EØS-terskelverdiene. *Lov og rett*, *47*(5-06), 361–379. https://doi-org.ezproxy.uis.no/10.18261/ISSN1504-3061-2008-05-06-05

Weisæt, L. & Kjeserud, R. (2007) *Ledelse ved kriser – en praktisk veileder*. Gyldendal Akademisk.

Øyvann, S. (2014, 3. september). «Skygge-it» truer it-avdelingen. *Computerworld.* https://www.cw.no/cloud-computing-enterprise-sikkerhet/skygge-it-truer-it-avdelingen/191953

Vedlegg 1 – informasjon til informanter og samtykkeskjema

Formål
I forbindelse med vår masteroppgave i Risk analysis and Governance ved Universitet i Stavanger, ønsker vi å gjennomføre intervju(er) med fagperson(er) i din virksomhet. Oppgaven omhandler cybersikkerhet, og hvordan man i kommunal sektor følger opp leverandører slik at sannsynligheten for leverandørkjedeangrep minimeres. Oppgaven har som formål å se leverandørkjedeangrep fra tre perspektiver; norske kommuner, kommunenes samarbeid med myndighetene og aktør(er) med faglig kunnskap om kommunenes arbeid med risiko og cybersikkerhet.

Hva innebærer det for deg å delta?
Dersom du velger å stille til intervju vil intervjuet ta for seg ulike spørsmål knyttet til problemstillingen. Det er mulighet for å se gjennom intervjuguiden før intervjuet dersom det er ønskelig. Intervjuet er estimert til ca. 45-60 minutter, men det kan avvike noe ut ifra hvor mye du som respondent deler på hvert enkelt spørsmål.

Konfidensialitet og lydopptak
Konfidensialitet etterstrebes, og alle informanter vil anonymiseres ved hjelp av kodenavn i teksten. På denne måten sikrer vi at opplysningene blir behandlet anonymt. Dersom det er ønskelig vil du også kunne få mulighet til å godkjenne tekst og sitat som brukes i oppgaven før den leveres endelig inn.
For å kunne gjengi pålitelige data og kvalitetssikre dine uttalelser er det ønskelig at vi benytter taleopptak under intervjuet. Dette for å unngå distraksjon ved å måtte ta notater, samt for å kunne delta aktivt i samtalen. Opptaket vil da kun lyttes til av oss i etterkant av intervjuet, og slettes så snart det er transkribert.

Det er frivillig å delta
Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine opplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke ønsker å delta, eller senere velger å trekke deg. Ved å signere denne erklæringen godtar du at opplysninger som gis under intervjuet kan benyttes videre i oppgaven.

Samtykkeerklæring
Jeg har mottatt og forstått informasjon om prosjektet «cybersikkerhet og risiko for leverandørkjedeangrep i kommunal sektor», og har fått anledning til å stille spørsmål.
Jeg samtykker til: ¨ å delta i intervju ¨ og at opplysningene som blir oppgitt under intervju kan benyttes anonymt videre i oppgaven. Jeg samtykker til at mine opplysninger behandles frem til prosjektet er avsluttet.
Jeg er kjent med at samtykket kan trekkes ved å sende kontakte Hans Tore Haagensen på telefon ******** eller mail: ********@stud.uis.no

Dato: Sted:

Signert deltaker

_____

Signert prosjektleder

_____

Vedlegg 2 – intervjuskjema kommuner

Innledning:
Fortelle om bakgrunnen for oppgaven og rammene rundt datainnhentingen

Problemstilling

- **Hvordan håndterer norske kommuner risikoen for cyberangrep via leverandørers IKT tjenester?**
- **Hvordan implementerer norske kommuner risiko og cybersikkerhet i anskaffelser?**
- **Hvordan opplever norske kommuner myndighetenes arbeid med risiko og cybersikkerhet?**

Databehandling:

- Det vil bli gjort lydopptak (informant må gjøre seg til kjenne på opptaket og klart gi sitt samtykke).
- Lydopptakene vil bli lagret så lenge det er praktisk nødvendig for så å bli slettet. En transkribering av lydopptakene vil bli gjort som en del av datauthentingen, analysen og struktureringen.
- Ingen navn eller stillingstitler vil bli gjengitt i oppgaven, men informasjon rundt virksomhetsoppgaver og kompetanse vil stedvis bli gjengitt.

Intervjuet:

- Cirka 1 times. varighet.
- Informantbasert med variasjonsutvelgelse.
- Fysisk/digitalt

Introspørsmål:

- Kan du si litt om virksomheten du representerer?
- Hva er tillingstittelen din og hva gjør du?
- Kan du si litt om erfarings-/kompetansebakgrunnen din?

Del 1 – Risiko

- Hvordan har kommunen/virksomheten organisert arbeidet med risiko? Fortell for eksempel om roller, mandat og beslutningsprosess.

- Hvordan har kommunen definert risiko?
    - Ulikt mellom fagområder?

- Benytter kommunen/virksomheten et rammeverk for risikostyring?
    - Om så, hvilket?
    - Hvordan brukes det i praksis?

- Har kommunen definert en risikoaksept?

    - Spesielt for cybersikkerhet?

- Hvordan opplever kommunen myndighetenes arbeid med risiko?

Del 2 – Cybersikkerhet

- Hvordan har kommunen/virksomheten organisert arbeidet med cybersikkerhet/informasjonssikkerhet? Fortell for eksempel om roller, mandat og beslutningsprosess.

- Benytter kommunen/virksomheten et rammeverk eller standard for cybersikkerhet?

- Er det gjort spesifikke tiltak for å forhindre cyberangrep?
    - Tekniske eller organisatoriske?
    - Mot leverandørkjedeangrep?

- Hvordan opplever du myndighetenes rolle når det gjelder forebyggende arbeid innenfor cybersikkerhet?

Del 3 – Anskaffelser

- Hvordan har kommunen/virksomheten organisert arbeidet med anskaffelser? Fortell for eksempel om roller, mandat og beslutningsprosess.

- Hvordan gjennomfører virksomheten anskaffelser?
    - Har virksomheten en etablert prosess?

- Hvordan vil du beskrive bestillerkompetanse ved anskaffelser av IKT tjenester?
    - Fokus på drift vs cybersikkerhet?

- Hvordan implementer kommunen/virksomheten cybersikkerhet i anskaffelser?
    - Standard tekniske krav?
    - Sertifisering av leverandør?

- Hvordan følger virksomheten opp cybersikkerhet hos leverandører under livsløpet og kontraktens levetid?
    - Krav til sikkerhet?
    - Evne til avvikshåndtering?
    - Rapportering?
    - Audit?
    - Reforhandlig?

- Er det spesielle utfordringer med hvordan dagens regelverk for anskaffelser?

- Er det noen spørsmål vi burde ha stilt?

Sluttkommentar: