Kontrollutvalget

Deres ref.:	Vår ref. (saksnr.):	Saksbeh.:	Dato:
	21/1123 - 77	Kari Breisnes, +47 91679943	04.04.2022

Oppfølging etter rapport 1/2019 Sikkerhetskrav i IKT-anskaffelser

Saken gjelder:
Kommunerevisjonen har gjennomført en oppfølgingsundersøkelse etter rapport 1/2019 *Sikkerhetskrav i IKT-anskaffelser*, jf. kontrollutvalgets vedtak 31. august 2021 sak (58). Undersøkelsen tilhører området virksomhetsstyring, digitalisering og informasjonssikkerhet, jf. bystyrets vedtak om *Overordnet analyse og plan for forvaltningsrevisjon og eierskapskontroll 2020–2024* av 21. oktober 2020 (sak 283).

I 2018–2019 gjennomførte Kommunerevisjonen en forvaltningsrevisjon for å undersøke om kommunen stiller gode og relevante sikkerhetskrav i anskaffelser på IKT-området. Anskaffelsene var foretatt av Bydel Alna, Bymiljøetaten, Barne- og familieetaten, Helseetaten, Utdanningsetaten og Utviklings- og kompetanseetaten.

Forvaltningsrevisjonen viste at virksomhetene for de fleste anskaffelsene hadde stilt informasjonssikkerhetskrav til systemene som ble anskaffet. I et flertall av anskaffelsene var det ikke gjennomført risikovurderinger av informasjonssikkerhet som kunne gi grunnlag for sikkerhetskrav. Videre var det svært begrenset sikkerhetstesting før systemene ble satt i drift. Samlet ett ga dette risiko for at sikkerheten i de anskaffede systemene ikke var i tråd med virksomhetens og kommunens behov.

I oppfølgingsundersøkelsen har Kommunerevisjonen sett på om virksomhetene og de ansvarlige byrådene/byrådsavdelingene har fulgt opp meldte tiltak og politiske føringer.

Basert på mottatte utsagn og gjennomgått dokumentasjon viste oppfølgingsundersøkelsen at Byrådsavdeling for miljø og samferdsel, Bymiljøetaten og Utviklings- og kompetanseetaten hadde iverksatt meldte tiltak og fulgt opp politiske føringer etter rapport 1/2019 *Sikkerhetskrav i IKT-anskaffelser*. Helseetaten hadde i hovedsak iverksatt meldte tiltak og fulgt opp politiske føringer.

Byrådsavdeling for finans, Byrådsavdeling for oppvekst og kunnskap, Barne- og familieetaten, Bydel Alna og Utdanningsetaten hadde delvis iverksatt meldte tiltak og fulgt opp politiske føringer. Byrådsavdeling for finans hadde blant annet ikke oppdatert alle maler eller utarbeidet en forenklet databehandleravtale og veiledere for å anskaffe skytjenester. Byrådsavdeling for finans oppga at utviklingen i trusselbildet og pandemiutbruddet ga behov for omprioritering og utsettelse av oppgaver. Byrådsavdeling for oppvekst og kunnskap hadde ikke bedt Barne- og familieetaten sikre at det fantes rutiner for risikovurdereringer og tilstrekkelig testing. Barne- og familieetaten hadde ikke ferdigstilt rutiner som skulle bidra til å sikre ROS-analyser, evaluering og testing. Bydel Alna hadde ikke ferdigstilt tiltak for å sørge for nødvendige kontroller og testing av sikkerhetskrav. Utdanningsetaten hadde ikke oppdatert rutiner med krav om å dokumentere evalueringen av sikkerhetskrav og sikkerhetstesting.

Byrådsavdeling for helse, eldre og innbyggertjenester hadde ikke fulgt opp anbefalingene fra rapport 1/2019 særskilt ovenfor Helseetaten og Bydel Alna, men viste til tiltak i styringsdialogen som kunne bidra til at anbefalingene ble fulgt opp.

Saksfremstilling:
I det følgende presenteres konklusjonene i rapport 1/2019 *Sikkerhetskrav i IKT-anskaffelser* og den politiske behandlingen av rapporten. Deretter presenteres resultatet av Kommunerevisjonens oppfølgingsundersøkelse.

1. Forvaltningsrevisjonen (rapport 1/2019)

Kommunerevisjonen undersøkte i 2018–2019 om kommunen stiller gode og relevante sikkerhetskrav i anskaffelser på IKT-området. Anskaffelsene var foretatt av Barne- og familieetaten, Bydel Alna, Bymiljøetaten, Helseetaten, Utdanningsetaten og Utviklings- og kompetanseetaten. Kommunerevisjonen så på om

- de aktuelle virksomhetene hadde vurdert behovet for sikkerhet i systemet som skulle anskaffes, og om
- krav til sikkerhet har blitt fulgt opp overfor leverandør fram til systemet var implementert.

Forvaltningsrevisjonen viste at virksomhetene for de fleste anskaffelsene hadde stilt informasjonssikkerhetskrav til systemene som ble anskaffet. I et flertall av anskaffelsene var det imidlertid ikke gjennomført risikovurderinger av informasjonssikkerhet som kunne gi grunnlag for sikkerhetskrav. Videre var det svært begrenset sikkerhetstesting før systemene ble satt i drift. Samlet sett ga dette risiko for at sikkerheten i de anskaffede systemene ikke var i tråd med virksomhetens og kommunens behov.

Kommunerevisjonen anbefalte at alle de reviderte virksomhetene burde vurdere tiltak som kunne gi større trygghet for at systemer som anskaffes, har et sikkerhetsnivå i tråd med virksomhetens behov. Særlig burde det sikres at virksomheten

- sørget for tilstrekkelige risikoanalyser som grunnlag for informasjonssikkerhetskrav i kravspesifikasjoner, og
- gjennomførte tilstrekkelig kontroll av at systemer som anskaffes, ivaretok sikkerhetsbehovene, herunder at det ble gjennomført egne sikkerhetstester ved vurdert behov.

Anbefalinger som gjaldt enkelte virksomheter:

- Barne- og familieetaten og Utdanningsetaten burde sørge for en tilfredsstillende evaluering av leverandørers tilbakemelding på sikkerhetskrav i kravspesifikasjoner.

- Bydel Alna burde sørge for tilstrekkelig kontroll med anskaffelsesprosessene slik at det ble stilt nødvendige risikobaserte krav til informasjonssikkerhet, at kravene ble evaluert på en tilfredsstillende måte og at det ble gjennomført nødvendige kontroller og testing av sikkerhetskrav før IT-systemer settes i drift.

Alle virksomhetene og de ansvarlige byråder/byrådsavdelinger varslet tiltak etter rapporten.

2. Politisk behandling av forvaltningsrevisjonen

Kontrollutvalget behandlet rapporten i møtet 29.01.2019 (sak 10), og vedtok følgende:

> Kontrollutvalget merker seg at Kommunerevisjonens rapport 1/2019 *Sikkerhetskrav i IKT-anskaffelser* viser at virksomhetene kun i et fåtall av de undersøkte anskaffelsene gjennomførte risikovurderinger av informasjonssikkerhet. I tillegg var det i de fleste tilfeller svært begrenset sikkerhetstesting før systemene ble satt i drift.
>
> Kontrollutvalget merker seg at alle virksomhetene har varslet flere tiltak etter rapporten. Utvalget understreker viktigheten av at det gjennomføres nødvendige tiltak, særlig knyttet til risikovurderinger og testing av systemene, slik at påpekt risiko for manglende sikkerhet reduseres. Mangelfull sikkerhet i et system kan føre til at konfidensielle opplysninger kommer på avveie, eller at virksomhetskritisk informasjon ikke er korrekt, går tapt eller ikke er tilgjengelig ved behov.
>
> Kontrollutvalget tar for øvrig Kommunerevisjonens rapport 1/2019 *Sikkerhetskrav i IKT-anskaffelser* til orientering.
>
> Saken sendes finanskomiteen.

Finanskomiteen behandlet rapporten 14.03.2019 (sak 39) og fattet vedtak i tråd med kontrollutvalgets vedtak.

3. Kommunerevisjonens oppfølgingsundersøkelse

Ifølge kommuneloven § 23-2 første ledd bokstav e), jf. forskrift om kontrollutvalg og revisjon § 5, skal kontrollutvalget påse at vedtak bystyret treffer ved behandlingen av forvaltningsrevisjonsrapporter, blir fulgt opp. Byrådet har ansvaret for oppfølgingen av bystyrets vedtak, jf. kommuneloven § 10-2 første ledd og § 13-1 fjerde ledd. Det ligger ikke til kontrollutvalget å fastsette hvordan administrasjonen skal følge opp påviste avvik/svakheter.

Kommunerevisjonen har undersøkt om tiltakene som ble varslet av de ansvarlige byråder/byrådsavdelinger og de reviderte virksomheter, er iverksatt, samt om føringer fra den politiske behandlingen av rapporten i bystyrets organer er fulgt opp. Når det gjelder politiske føringer, har Kommunerevisjonen lagt til grunn at det gjennomføres nødvendige tiltak, særlig knyttet til risikovurderinger og testing av systemene, slik at påpekt risiko for manglende sikkerhet reduseres.

Vi har gjennomført en enkel oppfølgingsundersøkelse i tråd med oppdraget fra kontrollutvalget. Oppfølgingsundersøkelsens innretning gjør at vi ikke har kunnet klarlegge effekten av tiltak og om de er tilstrekkelige. Da de meldte tiltakene er forskjellige mht. ambisjons- og detaljeringsnivå, kan dessuten en byråd eller virksomhet komme dårligere ut sammenlignet med andre, enn det som ville vært tilfellet ved en ny fullskala forvaltningsrevisjon.

Dataene er i hovedsak innhentet i perioden januar–februar 2022, og består av skriftlige redegjørelser og dokumentasjon. Virksomhetene og de ansvarlige byrådene har hatt mulighet til å komme med tilbakemelding på utkast til faktaframstilling og Kommunerevisjonens vurderinger.

I det følgende gjør vi nærmere rede for varslede tiltak etter forvaltningsrevisjonen, status på oppfølgingstidspunktet og Kommunerevisjonens vurderinger. Redegjørelsen er strukturert etter sektor.

3.1 Byrådsavdeling for finans

3.1.1 Meldte tiltak

Byråden for finans ville vurdere om kravene til informasjonssikkerhet var tilstrekkelige og godt nok forankret i virksomhetene. Informasjonssikkerhet og personvern ved IKT-anskaffelser var et av satsningsområdene for 2019 og ville omfatte alle fasene i anskaffelsesprosessen.

Byråden ville vurdere behovet for tiltak som kunne sørge for en bedre forankring av malen for databehandleravtale i virksomhetene slik at den i større grad ble tatt i bruk. Det ville også bli utarbeidet en forenkle versjon av malen for databehandleravtale.

Byråden oppga også at det i tildelingsbrevet for 2019 til Utviklings- og kompetanseetaten var stilt krav til at etaten, i samarbeid med byrådsavdelingen, skulle lage og oppdatere maler for kontraktstrategi, konseptutvalgsutredninger, behov- og kravspesifikasjon, avtaledokumenter og databehandleravtaler, slik at disse blant annet ivaretok hensynet til krav i ny sikkerhetslov. Etaten skulle også utarbeide en veileder for å anskaffe skytjenester, slik at behov og krav til personvern og informasjonssikkerhet ble ivaretatt. Etaten skulle videre utarbeide et sett av standardkrav til sikkerhetstester, samt maler og veiledere som skulle sikre at krav til ROS-analyser og personvernkonsekvensanalyser ble ivaretatt både i virksomheten og i prosjekter, samt hos alle leverandører og deres underleverandører.

Tiltakene skulle iverksettes fortløpende gjennom 2019 og 2020.

3.1.2 Status på oppfølgingstidspunktet

Forankring av krav til informasjonssikkerhet

Byrådsavdeling for finans la til grunn at kommunens instruks for informasjonssikkerhet ble etterlevd. For å forankre kravene skulle virksomhetsleder i 2019 og 2020 besvare om kravene til at virksomheten stilte gode og relevante personvern- og sikkerhetskrav i anskaffelser på IKT-området var ivaretatt i *Virksomhetsleders egenerklæring*. Virksomhetsleder skulle også besvare om kravet til at det ble foretatt risikovurderinger og personvernkonsekvensvurderinger i forkant av anskaffelsene og underveis var ivaretatt, og om det ble utført sikkerhetstester ut fra foreliggende behov. I erklæringen for 2021 var teksten i siste delsetning justert til å lyde «... og det blir utført sikkerhetstest og leverandørvurderinger der det er relevant».

Byrådsavdelingen oppga at rapporteringene i 2021 viste noe bedring, men også at det fortsatt var variasjoner og behov for oppmerksomhet på området. En egen standard for anskaffelser og leverandørforhold var på oppfølgingstidspunktet under utarbeidelse som en del av kommunens overordnede styringssystem for informasjonssikkerhet ifølge byrådsavdelingen.

Bruk av databehandleravtale

Byrådsavdelingen oppga at det var vurdert og iverksatt tiltak for å øke bruken av databehandleravtale. Kommunens egen mal for databehandleravtale ble revidert, men etter en ny vurdering ble Direktoratet for forvaltning og økonomistyrings mal for databehandleravtale valgt. Dette innebar ifølge byrådsavdelingen en forenkling av arbeidet for leverandørene. Videre var behovet for databehandleravtale inkludert i den veiledende sjekklisten for informasjonssikkerhet ved avslutning av prosjekter som resulterer i innføring av en ny tjeneste.

Byrådsavdelingen oppga at det var planlagt en aktivitet for utarbeiding av nye og forenklede maler, men at ferdigdato for disse ikke var berammet. Byrådsavdelingen vurderte at eksisterende mal hadde en rimelig god forankring i kommunen, men at en forenklet mal ville kunne medføre økt bruk og høyere kvalitet på databehandleravtaler.

Byrådsavdelingen oppga videre at virksomhetenes rapportering om bruken av databehandleravtaler i rapporteringene *Ledelsens gjennomgang* og *Virksomhetsleders egenerklæring* tydet på fortsatt bedring på området. Etter byrådsavdelingens vurdering hadde en strengere håndheving av GDPR fra Datatilsynet også medført en økt bevissthet om viktigheten av å inngå databehandleravtaler.

Oppfølging av krav stilt til Utviklings- og kompetanseetaten om utviklingsarbeid på området
Byrådsavdelingen hadde i 2019 en prosess for revisjon av maler knyttet til anskaffelsesprosessen. Behov for revisjon ble kartlagt i samarbeid med Utviklings- og kompetanseetaten, og det ble avholdt flere samarbeidsmøter om arbeidsdeling og framdrift underveis i prosessen. Det ble gjort endringer i malene for kontraktstrategi og databehandleravtaler med hensyn på personvern og informasjonssikkerhet. Ifølge Utviklings- og kompetanseetaten var rammene i kontraktstrategien førende for utarbeidelsen av øvrige konkurransedokumenter. Føringene ble derfor ikke inntatt særskilt i øvrige maldokumenter for konkurranse, jf. punkt 3.2.2.

Vedrørende krav i ny sikkerhetslov oppga byrådsavdelingen at den fortsatt ventet på informasjon fra Kommunal- og distriktsdepartementet for å avklare føringer og kriterier for hvilke systemer som er av avgjørende betydning for grunnleggende nasjonale funksjoner. Byrådsavdelingen viste til at slik det så ut, ville dette treffe så smalt at det ikke var naturlig å inkludere kravene fra sikkerhetsloven i generelle maler. Klassifiseringen av konfidensialitetsgraderte systemer var ikke vesentlig endret i ny sikkerhetslov og byrådsavdelingen forventet at disse systemene fortsatt ble behandlet særskilt i de virksomhetene det gjaldt. Malene for konseptutvalgsutredninger, behov- og kravspesifikasjon, avtaledokumenter var ikke oppdatert.

Veileder for anskaffelse av skytjenester
Byrådsavdelingen hadde selv, med bistand fra Utviklings- og kompetanseetaten, utarbeidet en veileder for anskaffelse av skytjenester. Ifølge byrådsavdelingen dekket veilederen etablering av skytjenester, noe som også ville være til hjelp ved anskaffelser. Veilederen ble publisert 6. desember 2021. Formålet med veilederen var å bidra til å sikre at det ikke tas i bruk infrastruktur eller plattform i skyen som medfører uakseptabel risiko for kommunens virksomhet når det gjelder informasjonssikkerhet og personvern.

Krav til sikkerhetstester og maler for ROS-analyser og personvernkonsekvensanalyser
Byrådsavdelingen oppga at ettersom omfang og innhold i sikkerhetstester varierte, var det ikke gjennomført tiltak med formål å standardisere selve testene. Byrådsavdelingen viste til at Utviklings- og kompetanseetaten hadde jobbet med standardisering av prosessen og veiledning i hvilke typer tester som var aktuelle i ulike situasjoner. Etaten hadde etablert tre forskjellige tjenester for sikkerhetstesting som var publisert i tjenestekatalogen. For realisering av disse tjenestene kunne etaten også benytte underleverandører i henhold til eksisterende rammeavtaler eller systemdriftsavtalen hvis kapasitets- eller kompetansebehov skulle tilsi det. Ifølge byrådsavdelingen var fordelen med en slik sentralisert tjeneste at Utviklings- og

kompetanseetatens kompetanse bidro til spesifisering av selve sikkerhetstestene og til tolkning av resultatene. I tillegg ble metodikken som benyttes, utprøvd.

Byrådsavdelingen viste videre til arbeidet med innføring og tilrettelegging av et overordnet styringssystem for informasjonssikkerhet for hele kommunen. Styringssystemet omhandler også personopplysningssikkerhet. Som en del av arbeidet er det utarbeidet metodikk og verktøy for gjennomføring av ROS-analyser, samt malverk og veiledere for gjennomføring av personvernvurderinger og personvernkonsekvensvurderinger (DPIA) i 2021. Byrådsavdelingen pekte på at gjennomføring av ROS-analyser og personvernkonsekvensvurderinger var en naturlig del av styringssystemet i de ulike virksomhetene i kommunen og at disse normalt ville omfatte både linjen og prosjekt, samt relasjonen til leverandører og underleverandører.

Annet
I tilbakemeldingen på Kommunerevisjonens utkast til oppfølgingsundersøkelsen viste byrådsavdelingen til at utviklingen i det eksterne trusselbildet på IKT-området og pandemiutbruddet hadde gjort det nødvendig å revurdere planer. Blant annet førte pandemien til at Teams og Office365 ble innført over ett år tidligere enn planlagt. Dette krevde store ressurser og resulterte i at enkelte andre oppgaver måtte vente. Dette gjaldt blant annet utarbeidelse av en egen forenklet mal for databehandleravtaler. Byrådsavdelingen understreket at det forelå en mal som ble benyttet selv om det ble løst på en annerledes måte enn opprinnelig meldt. De samme forholdene førte til forsinkelser i arbeidet med veiledere for skytjenester, ROS-analyser og personvernkonsekvensvurderinger.

3.1.3 Kommunerevisjonens vurdering
Byrådsavdeling for finans hadde delvis iverksatt meldte tiltak og fulgt opp politiske føringer. Byrådsavdelingen hadde ikke oppdatert malene for konseptutvalgsutredninger, behov- og kravspesifikasjon og avtaledokumenter i tråd med det som ble varslet. Krav til sikkerhetstester var ivaretatt på en noe annerledes måte enn opprinnelig meldt. Byrådsavdelingen hadde ikke utarbeidet en forenklet databehandleravtale. Veilederne for skytjenester ROS-analyser og personvernkonsekvensvurderinger ble først ferdigstilt i 2021. Kommunerevisjonen merker seg byrådsavdelingens opplysninger om at utviklingen i trusselbildet og pandemiutbruddet ga behov for omprioritering og utsettelse av oppgaver.

3.2 Utviklings- og kompetanseetaten

3.2.1 Meldte tiltak
Utviklings- og kompetanseetaten hadde iverksatt eller ville iverksette to tiltak basert på rapportens konklusjoner og anbefalinger. Etaten hadde etablert retningslinjer for anskaffelser i styringssystemet for informasjonssikkerhet for å sikre at tilstrekkelig krav til sikkerhet i IKT-anskaffelser var satt, forankret og kommunisert i organisasjonen.

Etaten planla å legge inn oppdatert veiledningstekst i malen for kontraktstrategien i *Veileder for anskaffelser i Oslo kommune*, slik at kravene til ivaretakelse og dokumentasjon av informasjonssikkerheten i IKT-anskaffelser kom tydeligere frem. Tiltaket var planlagt utført i løpet av første kvartal 2019.

3.2.2 Status på oppfølgingstidspunktet

Etablerte retningslinjer for anskaffelse i styringssystemet for informasjonssikkerhet

Utviklings- og kompetanseetatens styringssystem stilte krav til gjennomføring av risikoanalyser som grunnlag for informasjonssikkerhetskrav i kravspesifikasjoner, og til gjennomføring av sikkerhetstester ved behov.

Veiledningstekst i kontraktstrategien

Etaten hadde oppdatert veiledning i malen for kontraktstrategi slik at kravene til ivaretakelse og dokumentasjon av informasjonssikkerheten i IKT-anskaffelser kom tydeligere frem. Kravene fremkom i eget punkt i strategien. Oppdatert mal for kontraktstrategi ble ifølge etaten publisert 6. mai 2019.

Når det gjelder status på oppfølgingstidspunktet for Byrådsavdeling for finans' krav til Utviklings- og kompetanseetatens utviklingsarbeid på området, er dette beskrevet i pkt. 3.1.2.

3.2.3 Kommunerevisjonens vurdering

Utviklings- og kompetanseetaten hadde iverksatt meldte tiltak og fulgt opp politiske føringer.

3.3 Byrådsavdeling for helse, eldre og innbyggertjenester

3.3.1 Meldte tiltak

Daværende Byrådsavdeling for eldre, helse og arbeid oppga at rapportens anbefalinger ville bli lagt til grunn ved seinere anskaffelser.

3.3.2 Status på oppfølgingstidspunktet

Byrådsavdelingen hadde ikke fulgt opp anbefalingene fra rapport 1/2019 særskilt overfor Helseetaten og Bydel Alna. Byrådsavdelingen oppga at det i den årlige styringsdialogen var gitt tydelige føringer til virksomhetene om at gjeldende regler skulle følges. Det forelå ikke referater fra møter med Helseetaten eller Bydel Alna hvor dette fremkom. Byrådsavdelingen viste også til at det i rapporteringene *Ledelsens gjennomgang* og *Virksomhetsleders egenerklæring* ble gitt tydelige føringer på hva som var forventet også når det gjaldt IKT-anskaffelser. Disse rapporteringene, sammen med tildelingsbrev og utviklingssamtaler mellom kommunaldirektør og etats- og bydelsdirektører, var ifølge byrådsavdelingen sentrale oppfølgingsaktiviteter i den årlige styringsdialogen. Byrådsavdelingen viste til at status etter rapporteringene *Ledelsens gjennomgang* og *Virksomhetsleders egenerklæring* også ble behandlet i ledelsen og at det ble iverksatt tiltak på områder med et særskilt forbedringspotensial.

Egenerklæringene for Bydel Alna i 2020 og 2021 viste at punktet vedrørende informasjonssikkerhet ved anskaffelser var satt til gult nivå. Egenerklæringene viste videre at bydelen i 2020 ikke hadde utført sikkerhetstesting i noen av de fire anskaffelsene som var foretatt og at den i 2021 ikke hadde utført sikkerhetstesting i de to anskaffelsene som var foretatt. I rapporteringen for 2021 sa bydelen at den kunne bli bedre på å foreta risikovurderinger og personvernkonsekvensvurderinger i forkant av anskaffelsene. Bydelen har opplyst at det var et stykke igjen før kravet om å gjennomføre nødvendige kontroller og testing av sikkerhetskrav før IT-systemer ble satt i drift, jf. pkt. 3.5.2.

Egenerklæringene for Helseetaten i perioden 2020–2021 viste at punktet vedrørende anskaffelser var satt til grønt nivå. I erklæringen for 2020 var det ikke oppgitt hvor mange av anskaffelsene (fire anskaffelser) det var utført sikkerhetstester for. Det sto imidlertid i erklæringen at det var noe uklart for virksomhetens ledelse hva som mentes med spørsmålet.

Egenerklæringen for 2021 viste at etaten ikke hadde utført sikkerhetstester i noen av de fire anskaffelsene som var foretatt.

Byrådsavdelingen viste til at Helseetaten hadde ansvaret for å anskaffe og forvalte sektorovergripende systemer hvor systemeierskapet lå til kommunaldirektør i byrådsavdelingen. Etaten gjennomførte ifølge byrådsavdelingen anskaffelser i nært samarbeid med Utviklings- og kompetanseetaten, og i de siste årene gjennom et nært samarbeid med fagmiljøene innenfor informasjonssikkerhet og personvern i Byrådsavdeling for finans. Disse fagmiljøene ga råd og veiledning og ga opplæring der det ble etterspurt. Byrådsavdelingen oppga at Helseetaten holdt seg til gjeldende regelverk når det gjaldt anskaffelser.

Byrådsavdelingen hadde sammen med Byrådsavdeling for finans etablert et nettverk innenfor informasjonssikkerhet og personvern for å gi god faglig støtte til virksomhetene. Byrådsavdelingen påpekte at bydelenes anskaffelser utover samkjøpsavtaler var veldig begrenset og at det derfor var viktig at de benyttet kommunens anskaffelsesfaglige kompetanse i Utviklings- og kompetanseetaten og fagmiljøet i Byrådsavdeling for finans innenfor informasjonssikkerhet og personvern når de planla anskaffelser innenfor IKT området.

3.3.3 Kommunerevisjonens vurdering

Byrådsavdeling for helse, eldre og innbyggertjenester hadde ikke fulgt opp anbefalingene fra rapport 1/2019 særskilt overfor Helseetaten og Bydel Alna, men viste til tiltak i styringsdialogen som kunne bidra til at anbefalingene ble fulgt opp. Kommunerevisjonen merker seg at det i virksomhetsleders egenerklæring for de to undersøkte virksomhetene i sektoren fremkom svakheter på området. Det er ikke i tråd med de politiske føringene.

3.4 Helseetaten

3.4.1 Meldte tiltak

Helseetaten ville i større grad vektlegge risikovurderinger før utarbeidelse av krav til informasjonssikkerhet i forbindelse med anskaffelser, og også i større grad dokumentere hvilke vurderinger som var gjort knyttet til sikkerhetstesting før nye systemer ble satt i produksjon. Etaten skulle iverksette tiltakene i januar 2019.

3.4.2 Status på oppfølgingstidspunktet

Helseetaten oppga at den hadde gjennomført tre anskaffelser i 2019. Etaten var på oppfølgingstidspunktet også i ferd med å lyse ut konkurranse om en ytterligere anskaffelse. Etaten hadde gjennomført risikovurderinger av de tre anskaffelsene før utlysningen der kravene til informasjonssikkerhet fremgikk. Vurderingene var basert på Oslo kommunes metode for ROS-analyse.

Kravene til informasjonssikkerhet ble fulgt opp som en del av godkjenningsprøvene for de tre fullførte anskaffelsene. I godkjenningsprøvene vurderte egne team i etaten om IKT-systemene ivaretok sikkerhetskravene basert på dokumentasjon på og dialog med leverandørene. I to anskaffelser inngikk ikke sikkerhetstesting i godkjenningsprøvene. Det forelå ikke dokumenterte vurderinger av behovet for slik testing før systemene ble satt i drift. I den tredje godkjenningsprøven var det satt krav om at leverandør måtte utføre sikkerhetstest før systemet ble satt i drift. Slik test var utført.

Etaten oppga at den la bransjestandarden for helse- og omsorgssektoren, *Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren* (beskrevet og omtalt som

Normen i helse- og omsorgsbransjen*)* til grunn for kravene til informasjonssikkerhet og personvern som ble stilt i etatens anskaffelser. Normen stilte blant annet krav til at informasjonssikkerhet ved anskaffelser skulle inngå i virksomhetens styringssystem for informasjonssikkerhet, at kompetanseressurser innen informasjonssikkerhet skulle delta i anskaffelser og at krav skulle bygge på en dekkende risikovurdering. Normen stilte videre krav til at virksomheten sikret at relevante sikkerhetskrav inngikk i alle anskaffelser.

Helseetaten oppga at den arbeidet kontinuerlig for å forbedre rutinene for kravstilling i anskaffelser. For anskaffelsen etaten var i ferd med å utlyse hadde etaten vurdert at det ikke var tilstrekkelig at leverandørene bekreftet at de tilfredsstilte kravene i Normen, uten å utdype hvordan de oppfylte de enkelte kravene. Etatens personvernkoordinator og informasjonssikkerhetsteamet hadde derfor gjennomført en vurdering av samtlige krav i Normen. Disse var deretter omsatt i minimumskrav og evalueringskrav i kravspesifikasjonen for å sikre at etaten også fikk informasjon om underlaget leverandørene besvarte Normen ut i fra. Ifølge etaten var formålet med dette å stille tydeligere krav til leverandørene, sørge for at de gjorde et godt forarbeid og dermed redusere arbeidet med oppfølging av leverandørenes oppfyllelse av personvern og informasjonssikkerhetskrav i forbindelse med akseptansetestene.

3.4.3 Kommunerevisjonens vurderinger

Basert på utsagn og gjennomgått dokumentasjon er Kommunerevisjonens vurdering at Helseetaten i hovedsak hadde iverksatt meldte tiltak og fulgt opp politiske føringer. For to anskaffelser var det ikke dokumentert hvilke vurderinger som var gjort av behovet for sikkerhetstesting før systemene ble satt i drift

3.5 Bydel Alna

3.5.1 Meldte tiltak

Bydel Alna oppga at den allerede hadde satt i gang tiltak i samsvar med anbefalingene.

3.5.2 Status på oppfølgingstidspunktet

Bydel Alna oppga å ha stort fokus på at anskaffelser skulle foregå korrekt. Bydelen påpekte at den i stor grad benyttet Oslo kommunes samkjøpsavtaler. I de tilfeller bydelen måtte gjøre egne anskaffelser, ble i all hovedsak konkurransegjennomføringsverktøyet «KGV» lagt til grunn.

Bydelen oppga videre at IKT-seksjonen nå var involvert i de fleste IKT-anskaffelser, noe som ifølge bydelen sikret at det ble stilt risikovurderte krav til informasjonssikkerhet. Bydelen oppga at det imidlertid var et stykke igjen før kravet om å gjennomføre nødvendige kontroller og testing av sikkerhetskrav før IT-systemer settes i drift, ble tilfredsstilt. Samtidig påpekte bydelen at den i liten grad anskaffer egne IT-systemer ettersom den i all hovedsak var knyttet opp mot sentrale løsninger i Oslo kommune. Bydelen lente seg på Utviklings- og kompetanseetatens kompetanse og leveranse i de fleste systemer.

3.5.3 Kommunerevisjonens vurdering

Basert på bydelens utsagn er det Kommunerevisjonens vurdering at Bydel Alna delvis hadde gjennomført meldte tiltak og fulgt opp politiske føringer. Bydelen hadde ikke ferdigstilt tiltak for å sørge for nødvendige kontroller og testing av sikkerhetskrav før IT-systemer ble satt i drift.

3.6 Byråd for miljø og samferdsel

3.6.1 Meldte tiltak

Byråden ville i 2019 følge opp undersøkelsens konklusjoner og anbefalinger med Bymiljøetaten i styringsdialogen, og oppga at dette spesielt gjaldt anskaffelsene Prosjekthotell og Saksbehandlingsverktøy beboerparkering.

3.6.2 Status på oppfølgingstidspunktet

Oppfølging av om risikoanalyser legges som grunn for krav til informasjonssikkerhet

Byrådsavdeling for miljø og samferdsel fulgte opp at Bymiljøetaten hadde lukket avvikene i de to aktuelle IKT-anskaffelsene i etatsstyringsmøtet for 2. tertial i 2019. Byrådsavdelingen har videre fulgte opp etatens arbeid med informasjonssikkerhet og personvern gjennom de årlige rapporteringene *Ledelsens gjennomgang* og *Virksomhetsleders egenerklæring*. Byrådsavdelingen viste blant annet til at etaten i 2021 meldte at det ble utarbeidet risikovurderinger i forkant av anskaffelsene og at disse ble lagt til grunn i utarbeidelse av krav til leverandører. Det ble også meldt at etaten utførte sikkerhetstest og leverandørvurderinger der det var relevant. Bymiljøetaten rapporterte også i egenerklæringen at formalisering av rutiner gjensto og skulle gjennomføres høsten 2021.

Byrådsavdelingen viste også til at den fulgte opp etatens arbeid med informasjonssikkerhet, anskaffelser og internkontroll i styringsdialogen. Videre viste byrådsavdelingen til at den de siste årene hadde jobbet med å systematisere oppfølgingen av informasjonssikkerhet i underliggende etater, og at det i 2021 var arbeidet med å etablere akseptabelt risikonivå for sektoren som helhet. Dette arbeidet fortsatte ifølge byrådsavdelingen i 2022.

3.6.3 Kommunerevisjonens vurdering

Basert på dokumentasjon og byrådsavdelingens utsagn er det Kommunerevisjonens vurdering at Byrådsavdeling for miljø og samferdsels hadde iverksatt meldte tiltak og fulgt opp politiske føringer.

3.7 Bymiljøetaten

3.7.1 Meldte tiltak

Bymiljøetaten ville vurdere og eventuelt gjennomføre tiltak etter rapporten. Tiltakene ville konkretiseres nærmere i en plan hvor det ble sett hen til rapporten. Etaten vurderte å foreta justeringer som ivaretok rapportens påpekninger vedrørende rutiner for involvering og samarbeid på tvers av fagmiljøer ved IKT-relaterte anskaffelser. Etaten hadde satt i gang et arbeid for å utvikle ny anskaffelsesstrategi, som også ville også berøre forhold knyttet til kontraktsoppfølging og internkontroll. Rapportens funn ville bli vurdert også i denne prosessen.

Etaten ville gjennomgå rutiner og prosesser for å sikre konsistens i fremtidige anskaffelser med fokus på informasjonssikkerhet. Tiltakene ville gjennomføres i løpet av første halvår 2019.

3.7.2 Status på oppfølgingstidspunktet

Plan for iverksettelse av tiltak

Bymiljøetaten oppga at Kommunerevisjonens rapport var fulgt opp gjennom relevante tiltak utført etter følgende plan: å utvikle en anskaffelsesstrategi, å integrere risikovurderinger i anskaffelser som gjøres etter lov om offentlige anskaffelser og å styrke arbeidet i etaten med informasjonssikkerhet. Etaten oppga at den siden 2019 hadde jobbet målrettet med oppfølging av alle tre elementene i denne planen.

Etaten oppga at de tre punktene nevnt ovenfor allerede var aktiviteter avdelingene med ansvar for henholdsvis anskaffelser og informasjonssikkerhet arbeidet med da rapporten fra Kommunerevisjonen kom. Ettersom tiltakene da var under oppfølging, var det etter etatens vurdering ikke behov for ytterligere konkretisering.

Anskaffelsesstrategi, internkontroll og interne rutiner for IKT-anskaffelser
Bymiljøetaten hadde ferdigstilt en anskaffelsesstrategi datert juni 2019. Denne gjaldt anskaffelser generelt, og ikke IKT-anskaffelser spesielt. Strategien berørte forhold knyttet til kontraktsoppfølging og internkontroll. Etaten oppga at den i tråd med anskaffelsesstrategien hadde oppdatert og videreutviklet interne retningslinjer, maler og veiledning mv til bruk i anskaffelsesprosessene, herunder rutiner for å ivareta informasjonssikkerhet ved IKT-anskaffelser omtalt i rapport 1/2019. Retningslinjene og veiledningsmateriale var ifølge etaten tilgjengelig på Bymiljøetatens interne nettportal.

Rutinene som var utarbeidet for å vareta informasjonssikkerhet i anskaffelser, omfattet flere av temaene omtalt i rapport 1/2019, herunder anbefalingene om risikovurderinger og sikkerhetstester. Ifølge rutinene skulle det blant annet gjennomføres risikovurderinger for alle IKT-anskaffelser. Det skulle også stilles sikkerhetskrav i slike anskaffelser og det var stilt krav til testing av sikkerhetsfunksjonalitet. Etaten oppga at rutinene bidro til å ivareta informasjonssikkerheten ved IKT-anskaffelser og at den nå gjennomførte rutinemessig og løpende risikovurderinger i alle anskaffelser gjennomført etter lov om offentlige anskaffelser. Etaten viste til at vurderingene blant annet ble dokumentert i kontraktstrategien. Arbeidet med IKT-anskaffelser skjedde ifølge etaten i et internt samarbeid mellom ulike fagmiljøer som fagavdeling, avdeling med ansvar for digitalutvikling og avdeling for anskaffelse og entreprise.

3.7.3 Kommunerevisjonens vurdering

Basert på utsagn og gjennomgang av dokumentasjon er det Kommunerevisjonens vurdering at Bymiljøetaten hadde iverksatt meldte tiltak og fulgt opp politiske føringer. Kommunerevisjonen merker seg at Bymiljøetaten etter en vurdering ikke så behov for å utarbeide ytterligere konkretisering av tiltak for oppfølging av revisjonen slik som opprinnelig meldt etter forvaltningsrevisjonen i 2019.

3.8 Byråd for oppvekst og kunnskap

3.8.1 Meldte tiltak
Byråden for oppvekst og kunnskap ville følge opp undersøkelsen i den formelle styringsdialogen med Utdanningsetaten og Barne- og familieetaten i 2019 for å sikre at anbefalingene ble lagt til grunn i fremtidige anskaffelser. Byråden ville be virksomhetene sikre at det fantes rutiner for å gjennomføre risikovurderinger i forkant av IKT-anskaffelser og at det ble gjennomført tilstrekkelig testing og kontroll av at sikkerhetskravene var levert før nye løsninger ble satt i produksjon.

3.8.2 Status på oppfølgingstidspunktet
Byrådsavdeling for oppvekst og kunnskap oppga at den fulgte opp Utdanningsetatens og Barne- og familieetatens arbeid med informasjonssikkerhet og personvern gjennom den årlige rapporteringen av *Ledelsens gjennomgang* og *Virksomhetsleders egenerklæring*. Erklæringen inneholdt også rapportering av status for krav knyttet til anskaffelser. Status på dette området

var ifølge byrådsavdelingen derfor en del av den årlige oppfølgingen av rapporteringen og inngikk i styringsdialogen med etatene.

I 2019 var rapporteringen ifølge byrådsavdelingen tema på høstens etatsstyringsmøter for begge etatene. Etter etatsstyringsmøtet den høsten avholdt byrådsavdelingen et eget møte med Utdanningsetaten om informasjonssikkerhet og personvern hvor etaten blant annet redegjorde for status på tiltak knyttet til anbefalingene i Kommunerevisjonens rapport 1/2019. Byrådsavdelingen oppga at den innførte en praksis med et eget møte om informasjonssikkerhet og personvern i forbindelse med rapporteringene i 2019 for Utdanningsetaten og i 2020 for Barne- og familieetaten.

Vedrørende rutiner for risikovurderinger og sikkerhetstesting, viste referatet fra møtet i november 2019 at Utdanningsetaten skulle oppdatere etatens retningslinjer knyttet til anskaffelser med krav om risikovurderinger som grunnlag for relevante sikkerhetskrav i løpet av november. Byrådsavdelingen oppga at den gjennom dialogen med etaten forsto at rutiner i tråd med anbefalingene fra revisjonsrapporten ble ferdigstilt som planlagt. Byrådsavdelingen oppga at den hadde fulgt opp det varslede tiltaket om sikkerhetstesting selv om det ikke fremkom av møtereferatet. Som det fremgår av 3.9 nedenfor, hadde Utdanningsetaten på oppfølgingstidspunktet ikke egne rutiner for sikkerhetstesting ved IKT-anskaffelser.

Det kom ikke frem av referater etter etatsstyringsmøtene med Barne- og familieetaten om byråden har bedt etaten om å sikre at det fantes rutiner for risikovurderinger og testing og kontroll av sikkerhetskrav eller om etaten hadde etablert slike rutiner. Byrådsavdelingen kunne heller ikke vise til at dette var tatt opp med etaten på annen måte.

Barne- og familieetaten startet i desember 2021 med å utarbeide rutiner for anskaffelse av IKT-systemer, jf. pkt. 3.10.2 nedenfor. Ifølge rutinene skulle det blant annet gjennomføres ROS-Analyse for å identifisere sikkerhetsbehov, evaluering av sikkerhets- og personvernkrav av tilbud og test av sikkerhet og personvern ved leveranse. Rutinene var på oppfølgingstidspunktet ikke vedtatt.

3.8.3 Kommunerevisjonens vurdering

Byrådsavdeling for oppvekst og kunnskap hadde delvis iverksatt meldte tiltak og fulgt opp politiske føringer. Byrådsavdelingen hadde ikke bedt Barne- og familieetaten sikre at det fantes rutiner for risikovurderinger og tilstrekkelig testing. Etablering av rutiner var fulgt opp gjennom styringsdialogen med Utdanningsetaten. Som det fremgår av punkt 3.9 hadde Utdanningsetaten imidlertid ikke rutiner for sikkerhetstesting. Barne- og familieetaten hadde verken etablert rutiner for risikovurdering eller for sikkerhetstesting på oppfølgingstidspunktet, jf. punkt 3.10.

3.9 Utdanningsetaten

3.9.1 Meldte tiltak

Utdanningsetaten hadde iverksatt eller ville iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger, blant annet ville etaten oppdatere anskaffelsesrutinene for å sikre ensartede risikovurdering av informasjonssikkerhet i forkant av anskaffelser. Rutinene ville også oppdateres med krav om å dokumentere evalueringen av oppfyllelse av sikkerhetskravene, samt for å sikre tilstrekkelig kvalitet på sikkerhetstesting før produksjonssetting. Rutinene ville oppdateres innen første kvartal 2019.

3.9.2 Status på oppfølgingstidspunktet

Rutiner for anskaffelser

Utdanningsetaten oppga at rutiner på anskaffelsesområdet var oppdatert 9. februar 2021. Det var blant annet tatt inn et eget punkt i etatens anskaffelsesveileder om at IKT-anskaffelser over 1, 3 millioner kroner skulle godkjennes av IKT-avdelingen. Etaten viste videre til at den benyttet kommunens felles maler på området og at malene for behovsmelding og kontraktstrategi var de to vanligste som ble benyttet. Etaten viste til at kontraktstrategien inneholdt krav til informasjonssikkerhet. Malen inneholdt videre en matrise for risikovurderinger. Etaten oppga videre at det var gjennom behovsavklaringsaktiviteter og i kontraktstrategien det ble etablert krav til informasjonssikkerhet og testing ved IKT-anskaffelser. Anskaffelsens art var ifølge etaten retningsgivende for hvilken type risikovurdering som ble gjennomført.

Rutiner for sikkerhetskrav og sikkerhetstesting

Etaten hadde ikke rutiner som omtalte krav om å dokumentere evalueringen av sikkerhetskrav eller sikkerhetstesting ved IKT-anskaffelser. Etaten oppga at den alltid gjennomførte en konkret vurdering basert på risikoanalysen om hva slags sikkerhetstesting som skulle gjennomføres innen produksjonssetting. Valg av tilnærming var også avhengig av hvor tjenesten skulle driftes. Dette ettersom det kunne være en del forskjeller avhengig av om det var en skyløsning eller en internt driftet løsning. Kravene til sikkerhetstesting ble ifølge etaten beskrevet i kontraktgrunnlaget ved kjøp med avtaleformen SSA-T (kjøp av programvare som skal utvikles eller tilpasses for kunden dersom kunden ikke på forhånd kan spesifisere nøyaktig hvordan programvaren skal utvikles/tilpasses). SSA-T ble ifølge etaten benyttet ved utvikling eller større tilpasninger for IKT-systemer. Etaten oppga at all evaluering av krav i et tilbud ble dokumentert og at dette også gjaldt informasjonssikkerhetskravene. Etaten viste videre til at den hadde skriftlige rutiner for testing ved endringsprosesser ved funksjonelle endringer som den mente også var gjeldende ved anskaffelser.

3.9.3 Kommunerevisjonens vurdering

Basert på utsagn og gjennomgang av dokumentasjon er det Kommunerevisjonens vurdering at Utdanningsetaten delvis hadde iverksatt meldte tiltak og fulgt opp politiske føringer. Anskaffelsesrutinene ble oppdatert seinere enn meldt. Etaten hadde ikke oppdatert rutiner med krav om å dokumentere evalueringen av sikkerhetskrav og sikkerhetstesting ved anskaffelse av IKT-anskaffelser.

3.10 Barne- og familieetaten

3.10.1 Meldte tiltak

Barne- og familieetaten ville umiddelbart sikre at det ble gjennomført ROS-analyser før gjennomføring av anskaffelser, samt forbedre evaluering og testing av sikkerhetskrav ved fremtidige IKT-anskaffelser. Etaten ville i løpet av første halvår 2019 vurdere å gjennomføre ny sikkerhetstesting av den aktuelle anskaffelsen.

3.10.2 Status på oppfølgingstidspunktet

Etaten utarbeidet i desember 2021 et utkast til rutiner for anskaffelse av IKT-utstyr. Ifølge rutinene skulle det blant annet gjennomføres ROS-analyse for å identifisere sikkerhetsbehov, evaluering av sikkerhets- og personvernkrav av tilbud og test av sikkerhet og personvern ved leveranse. Det var ikke gitt nærmere beskrivelse av hvordan dette skulle utføres. Rutinene var på oppfølgingstidspunktet ikke vedtatt.

Etaten gjennomførte sikkerhetstesting av den aktuelle IKT-anskaffelsen. Endelig rapport etter testingen forelå mars 2020.

3.10.3 Kommunerevisjonens vurdering

Barne- og familieetaten hadde delvis fulgt opp meldte tiltak og politiske føringer. Etaten hadde gjennomført sikkerhetstesting av den aktuelle anskaffelsen, men det forelå ikke vedtatte rutiner for anskaffelse av IKT-utstyr. Slike rutiner vil kunne bidra til å sikre at det utføres ROS-analyser før IKT-anskaffelser og samt til å forbedre evaluering og testing av sikkerhetskrav ved fremtidige IKT-anskaffelser.

4. Kommunerevisjonens konklusjon

Kommunerevisjonens konklusjon er basert på mottatte utsagn og gjennomgått dokumentasjon. Oppfølgingsundersøkelsen viste at Byrådsavdeling for miljø og samferdsel, Bymiljøetaten og Utviklings- og kompetanseetaten hadde iverksatt meldte tiltak og fulgt opp politiske føringer etter rapport 1/2019 *Sikkerhetskrav i IKT-anskaffelser*.

Helseetaten hadde i hovedsak iverksatt meldte tiltak og fulgt opp politiske føringer, men for to anskaffelser var vurderingene av behovet for sikkerhetstesting ikke dokumentert.

Byrådsavdeling for finans, Byrådsavdeling for oppvekst og kunnskap, Barne- og familieetaten, Bydel Alna og Utdanningsetaten hadde delvis iverksatt meldte tiltak og fulgt opp politiske føringer. Byrådsavdeling for finans hadde blant annet ikke oppdatert alle maler eller utarbeidet en forenklet databehandleravtale og veiledere for å anskaffe skytjenester. Byrådsavdeling for finans oppga at utviklingen i trusselbildet og pandemiutbruddet ga behov for omprioritering og utsettelse av oppgaver. Byrådsavdeling for oppvekst og kunnskap hadde ikke bedt Barne- og familieetaten sikre at det fantes rutiner for risikovurderinger og tilstrekkelig testing. Barne- og familieetaten hadde ikke ferdigstilt rutiner som skulle bidra til å sikre ROS-analyser, evaluering og testing. Bydel Alna hadde ikke ferdigstilt tiltak for å sørge for nødvendige kontroller og testing av sikkerhetskrav. Utdanningsetaten hadde oppdatert anskaffelsesrutinene seinere enn meldt og ikke oppdatert rutiner med krav om å dokumentere evalueringen av sikkerhetskrav og sikkerhetstesting.

Byrådsavdeling for helse, eldre og innbyggertjenester hadde ikke fulgt opp anbefalingene fra rapport 1/2019 særskilt ovenfor Helseetaten og Bydel Alna, men viste til tiltak i styringsdialogen som kunne bidra til at anbefalingene ble fulgt opp.

At flere virksomheter ikke har iverksatt meldte tiltak og ikke fulgt opp politiske føringer kan gi risiko for at sikkerheten i anskaffede IKT-systemer ikke er i tråd med virksomhetenes og kommunens behov. Mangelfull sikkerhet i et system kan føre til at konfidensielle opplysninger kommer på avveie, eller at virksomhetskritisk informasjon ikke er korrekt, går tapt eller ikke er tilgjengelig ved behov.

Med hilsen

Unn H. Aarvold
kommunerevisor

Hilde Ludt
ass. avdelingsdirektør

Mottakere:
Kontrollutvalget