Oslo kommune
**Kommunerevisjonen**

Rapport 01/2019

# Sikkerhetskrav i IKT-anskaffelser

2019

Kommunerevisjonen – integritet og verdiskaping

# Tidligere publikasjoner fra Kommunerevisjonen i Oslo

**Rapport 01/2018 Svømmeopplæringen i barneskolen**
**Rapport 02/2018 Eierskapskontroll – Vigo IKS**
**Rapport 03/2018 Oppsummering av utvalgte undersøkelser gjennomført i regnskapsrevisjonen 2017**
**Rapport 04/2018 Renovasjonsetatens anskaffelse av avfallsinnhenting**
**Rapport 05/2018 Sykehjemsetaten – kvalitetsutvikling i langtidshjem og helsehus**
**Rapport 06/2018 Overordnet styring av informasjonssikkerhet**
**Rapport 07/2018 Saksbehandlingstid reguleringsplaner – Detaljregulering i Oslo kommune**
**Rapport 08/2018 Barnevernsinstitusjoner – kompetanse og bemanning m.m.**
**Rapport 09/2018 Bydelenes forebygging av utenforskap blant barn og unge**
**Rapport 10/2018 Måloppnåelse og resultater i Områdeløft Tøyen**
**Rapport 11/2018 Styring av Boligbygg Oslo KF for å forebygge korrupsjon og misligheter**
**Rapport 12/2018 Eiendomstransaksjoner i Boligbygg Oslo KF**
**Rapport 13/2018 Eierskapskontroll – HAV Eiendom AS**
**Rapport 14/2018 Klimaetatens arbeid med kommunens klimamål**
**Rapport 15/2018 Rehabilitering i helsehus**
**Rapport 16/2018 Ernæringsarbeidet i hjemmetjenesten**
**Rapport 17/2018 Spesialundervisning i videregående skole – Elvebakken videregående skole og Kuben videregående skole**
**Rapport 18/2018 Internkontroll i investeringsprosjekter i Omsorgsbygg**

**For mer informasjon om Kommunerevisjonen og våre rapporter se www.krv.oslo.kommune.no**

# Forord

Denne rapporten er et resultat av forvaltningsrevisjonsprosjektet om sikkerhetskrav i IKT-anskaffelser. Rapporten har også en deskriptiv del om blant annet virksomhetenes vurdering av leverandørenes modenhet og virksomhetenes informasjonssikkerhets-kompetanse i anskaffelsesprosjektene.

Undersøkelsen er forankret i kontrollutvalgets vedtak av 30.01.2018 (sak 7), og tilhører området anskaffelser, kontraktsoppfølging og tiltak mot arbeidslivskriminalitet jf. bystyrets vedtak om *Overordnet analyse og plan for forvaltningsrevisjon* 2016–2020 av 22.06.2016 (sak 186).

Forvaltningsrevisjon er en lovpålagt oppgave for Oslo kommune. Formålet med forvaltningsrevisjon er nedfelt i kommuneloven § 77 nr. 4:

> (…) systematiske vurderinger av økonomi, produktivitet, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak og forutsetninger (forvaltningsrevisjon).

Forvaltningsrevisjon i Oslo kommune gjennomføres iht. gjeldende standard for forvaltningsrevisjon i kommuner og fylkeskommuner i Norge (RSK 001).

Prosjektet er gjennomført av seniorrådgiver Atle Refsdal, seniorrådgiver Stig Eliassen og seniorrådgiver Morten A. Engebretsen. Sistnevnte var prosjektleder.

Vi vil takke Bydel Alna, Bymiljøetaten, Helseetaten, Barne- og familieetaten, Utviklings- og kompetanseetaten, Utdanningsetaten og berørte byrådsavdelinger for nødvendig bistand i løpet av prosjektet.

10.01.2019

Hilde Ludt
assisterende avdelingsdirektør

Morten A. Engebretsen
seniorrådgiver

# Innhold

# Hovedbudskap

Kommunerevisjonen har gjennomført en forvaltningsrevisjon av sikkerhetskrav i 15 IKT-anskaffelser. Anskaffelsene var foretatt av Bydel Alna, Bymiljøetaten, Barne- og familieetaten, Helseetaten, Utdanningsetaten og Utviklings- og kompetanseetaten.

Undersøkelsen viser at virksomhetene for de fleste anskaffelsene hadde stilt informasjonssikkerhetskrav til systemene som ble anskaffet. I et flertall av anskaffelsen 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 sett ga dette risiko for at sikkerheten i de anskaffede systemene ikke var i tråd med virksomhetenes og kommunens behov.

# Sammendrag

Oslo kommune er stadig mer avhengig av IKT-systemer i styring, forvaltning og drift av kommunens virksomhet. Systemene er ofte kritiske for at kommunen og den aktuelle virksomheten skal nå sine mål, og mange inneholder sensitiv informasjon. Flere viktige systemer er anskaffet de senere årene, og flere systemer er planlagt skiftet ut framover.

Formålet med undersøkelsen har vært å gi informasjon om status når det gjelder sikkerhetskrav i IKT-anskaffelser, og således bidra til forbedringer i kommunens arbeid på området.

Undersøkelsen har hatt følgende problemstilling:

- Stiller kommunen gode og relevante sikkerhetskrav i anskaffelser på IKT-området?

Problemstillingen er i hovedsak besvart gjennom følgende underproblemstillinger:

- Har de aktuelle virksomhetene vurdert behovet for sikkerhet i systemet som skal anskaffes?
- Har krav til sikkerhet blitt fulgt opp overfor leverandøren fram til systemet er implementert?

Undersøkelsen gir også informasjon om:

- virksomhetenes vurderinger av leverandørenes modenhet og evne til å levere i henhold til krav på informasjonssikkerhetsområdet,
- det er benyttet særskilt informasjonssikkerhetskompetanse i anskaffelser på IKT-området og
- eiendomsrett til data og systemer har blitt kontraktsregulert.

Kommunerevisjonen har undersøkt 15 anskaffelser i 6 virksomheter. For å sikre undersøkelsens relevans ble kun nyere anskaffelser valgt ut. Anskaffelsene ble videre valgt ut for å sikre en bredde av typer systemer, det være seg skytjenester, større fagsystemer og mer begrensede applikasjoner. Virksomhetene ble valgt ut for å dekke variasjon i erfaring med IKT-anskaffelser.

Revisjonskriteriene er i hovedsak utledet av tidligere personopplysningslov med forskrift, eForvaltningsforskriften og Oslo kommunes overordnede styringsdokumenter for ivaretakelse av informasjonssikkerhet.

Datagrunnlaget i undersøkelsen har i hovedsak bestått av dokumentasjon og redegjørelser fra virksomhetene om de valgte IKT-anskaffelsene.

I det følgende presenteres Kommunerevisjonens sentrale vurderinger.

***Utviklings- og kompetanseetaten***
Det var utarbeidet risikoanalyser forut for kravspesifikasjon for én av de tre undersøkte anskaffelsene. For en av de øvrige ble det heller ikke utarbeidet risikoanalyse senere. For den tredje ble det gjennomført en risikoanalyse etter at sikkerhetskrav var utarbeidet.

For alle tre anskaffelser var det stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Etaten hadde evaluert leverandørens tilbakemeldinger på kravene, men det var ikke gjennomført sikkerhetstester eller annen kontroll av sikkerhetskrav frem til iverksetting. Etaten hadde dermed ikke et tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet i systemene var ivaretatt.

***Helseetaten***
Det var utarbeidet risikoanalyser forut for kravspesifikasjon for én av de tre undersøkte anskaffelsene. For en av de øvrige ble det heller ikke utarbeidet risikoanalyse senere.

For alle tre anskaffelser var det stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. En av anskaffelsene hadde i undersøkelsesperioden kommet så langt at etaten hadde mottatt leverandørenes tilbakemeldinger på krav til informasjonssikkerhet. For denne anskaffelsen hadde Helseetaten vurdert leverandørens tilbakemeldinger. Etaten hadde gjennomført enkelte sikkerhetstester og annen kontroll av sikkerhetskrav for dette systemet frem til driftsettelse. Kommunerevisjonen stiller spørsmål om ytterligere kontroll burde vært gjennomført for å få tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet var ivaretatt.

***Bymiljøetaten***
Det var utarbeidet risikoanalyser forut for kravspesifikasjon for to av de tre undersøkte anskaffelsene.

For alle tre anskaffelser var det stilt flere krav til informasjonssikkerhet i kravspesifikasjonen, og etaten hadde også evaluert leverandørenes tilbakemeldinger på kravene, i tråd med revisjonskriteriene i denne rapporten. For ett av systemene tydet dokumentasjon fra etaten på at det var testet eller kontrollert at systemet overholdt stilte krav til informasjonssikkerhet. For ett annet av systemene stiller Kommunerevisjonen spørsmål ved at dette ikke var gjort. For det tredje systemet ble flere alvorlige sikkerhetssvakheter avdekket av Utviklings- og kompetanseetaten i sikkerhetstester etter at systemet var tatt i bruk. For dette systemet mener Kommunerevisjonen at etatens kontroll i forkant var mangelfull.

***Barne- og familieetaten***
Det var ikke utarbeidet risikoanalyse forut for kravspesifikasjon i den ene anskaffelsen som ble undersøkt. Dette ble imidlertid gjort senere i anskaffelsen.

Det var stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Leverandørens tilbakemelding på kravene var blitt evaluert, men leverandørens løsningsforslag var svært lite detaljert. Kommunerevisjonen anser derfor at etatens evaluering i for stor grad baserte seg på leverandørens vurderinger. Når det gjelder sikkerhetstesting, hadde etaten feilaktig lagt til grunn at Utviklings- og kompetanseetaten gjennomførte slike tester.

Kommunerevisjonen mener derfor at ytterligere kontroll burde vært gjennomført for å få tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet i systemet var ivaretatt.

***Utdanningsetaten***
Det var ikke utarbeidet risikoanalyser forut for kravspesifikasjon for noen av de tre undersøkte anskaffelsene. Etaten pekte på forhold som kunne bidra til å forklare dette, som for eksempel at etatens standard sikkerhetskrav var lagt til grunn for utforming av sikkerhetskravene til systemet som ble anskaffet. Det forelå imidlertid ikke dokumenterte vurderinger av om kravene faktisk dekket virksomhetens behov i den enkelte anskaffelse.

For alle tre anskaffelser var det stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. For én av anskaffelsene var det en svakhet at etaten ikke hadde gjennomført skriftlig evaluering av alle sikkerhetskravene. For en annen av anskaffelsene var det en svakhet at det ikke var gjennomført testing eller annen kontroll av sikkerhetskrav frem til driftsettelse. For den siste av anskaffelsene stiller Kommunerevisjonen spørsmål om det var gjennomført tilstrekkelig kontroll og testing av kravene. Anskaffelsen var ikke kommet langt nok til at Kommunerevisjonen kan konkludere.

***Bydel Alna***
Det var etter Kommunerevisjonens vurdering vesentlige mangler og svakheter ved sikkerhetskravene i de to undersøkte anskaffelsene. Det var ikke foretatt risikoanalyse i anskaffelsene. I én av anskaffelsene manglet sikkerhetskrav, og det var ikke blitt foretatt sikkerhetstester eller andre former for kontroll av informasjonssikkerhet før driftsettelse. Bydel Alna hadde ikke gjennomført nødvendige prosesser for å sikre at IT-systemene hadde sikkerhet i tråd med bydelens behov.

***Samlet vurdering***
Undersøkelsen viser at virksomhetene for de fleste anskaffelsene hadde stilt informasjons-sikkerhetskrav til systemene som ble anskaffet. Imidlertid hadde virksomhetene i et fåtall av de undersøkte anskaffelsene gjennomført risikovurderinger av informasjonssikkerhet som kunne gi grunnlag for sikkerhetskravene. Etter Kommunerevisjonens vurdering innebærer dette at flere av de undersøkte virksomhetene ikke hadde sørget for tilfreds-stillende prosesser som grunnlag for gode og relevante sikkerhetskrav. I tillegg var det i liten grad gjennomført sikkerhetstesting før systemene ble satt i drift. Det var også enkelte andre svakheter. Samlet gir dette risiko for at sikkerheten i de anskaffede systemene ikke var 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 tilgjengelige ved behov.

### *Anbefalinger*

Anbefalinger som gjelder alle de reviderte virksomhetene:

- Virksomhetene bør vurdere tiltak som kan gi større trygghet for at systemer som anskaffes har et sikkerhetsnivå i tråd med virksomhetens behov. Særlig bør det sikres at virksomheten har
  - sørget for tilstrekkelige risikoanalyser som grunnlag for informasjons-sikkerhetskrav i kravspesifikasjoner, og
  - gjennomført tilstrekkelig kontroll av at systemer som anskaffes ivaretar sikkerhetsbehovene, herunder at det er gjennomført egne sikkerhetstester ved vurdert behov.

Anbefalinger som gjelder enkelte virksomheter:

- Barne- og familieetaten og Utdanningsetaten bør sørge for en tilfredsstillende evaluering av leverandørers tilbakemelding på sikkerhetskrav i kravspesifikasjoner.
- Bydel Alna bør sørge for tilstrekkelig kontroll med anskaffelsesprosessene slik at det stilles nødvendige risikobaserte krav til informasjonssikkerhet, at kravene evalueres på en tilfredsstillende måte og at det gjennomføres nødvendige kontroller og testing av sikkerhetskrav før IT-systemer settes i drift.

### *Uttalelser til rapporten*

Rapporten ble 20.11.2018 sendt til uttalelse til Utviklings- og kompetanseetaten, Helseetaten, Bymiljøetaten, Barne- og familieetaten, Utdanningsetaten og Bydel Alna. I tillegg fikk ansvarlige byråder rapporten til uttalelse. Alle reviderte virksomheter har varslet tiltak etter rapporten. Uttalelsene er oppsummert og kommentert i kapittel 10. Alle uttalelsene er som helhet lagt som vedlegg 4 til rapporten. Tilbakemeldingene fra reviderte har et par steder medført endringer i rapporten. Rapportens hovedbudskap, konklusjon og anbefalinger er ikke blitt endret. Ved korrekturlesing av rapporten ble det avdekket en unøyaktighet i sammendraget som nå er rettet.

# 1. Innledning

## 1.1 Bakgrunn

Oslo kommune benytter et stort antall IKT-systemer. Mange viktige systemer er anskaffet de senere årene, og flere er planlagt skiftet ut framover. Behandling av informasjon er en sentral del av aktiviteten i det aller meste av virksomheten i Oslo kommune. Bruk av IKT skal bidra til økt tjenestekvalitet og effektivisering. Dette innebærer at kvaliteten på informasjonen og informasjonsbehandlingen er avgjørende for at kommunen og dens virksomheter skal nå sine mål. Videre forvalter og behandler kommunen informasjon som er underlagt lov- og forskriftskrav om beskyttelse, som helseopplysninger og andre personopplysninger, konkurransesensitiv informasjon og opplysninger som er av betydning for viktige samfunnsfunksjoner og vår sikkerhet.

For å sikre virksomhetenes informasjonsverdier er det viktig å stille gode sikkerhetskrav til leverandørene når IKT-systemer anskaffes og følge opp at disse kravene oppfylles. Kommunerevisjonen har tidligere gjennomført flere revisjoner av informasjons-sikkerhet. Erfaringene viser at manglende krav kan skyldes at kommunens virksomheter i varierende grad har kompetanse på og prioriterer informasjonssikkerhet som en integrert del av sin virksomhetsstyring og internkontroll. Dette kan i så fall resultere i at virksomheter ikke kjenner og har kontroll på sikkerheten i systemene. I neste omgang kan dette gi risiko for at det oppstår feil, at viktige funksjoner blir utsatt for sabotasje, og for at sensitive opplysninger kommer på avveie.

For at kommunen skal kunne nå sine mål og følge lover og regler, er det derfor viktig å sikre informasjonens

- tilgjengelighet, det vil si at informasjonen er tilgjengelig ved behov,
- integritet, det vil si at informasjonen ikke kan endres utilsiktet eller av uvedkommende,
- konfidensialitet, det vil si at informasjonen ikke skal bli kjent for uvedkommende.

Kravene som stilles for å sikre dette kan være av både teknisk, fysisk og organisatorisk art. Sikkerhetskrav omfatter blant annet regelverkskrav, krav til tilgjengelighet til informasjon og prosesser, teknisk sikkerhet i løsningen, tilgangsstyring og håndtering av data.

Ikke all informasjon og systemer har samme behov for beskyttelse. Nivået på informasjonssikkerhet bør følge av en konkret vurdering av risikoen som er knyttet til systemene og informasjonen som behandles. Sikkerhetskrav bør derfor ta utgangspunkt i målsettingen med systemanskaffelsen og tilpasses de iboende risikoer som kan true måloppnåelsen.

## 1.2 Formål og problemstillinger

Formålet med undersøkelsen har vært å gi informasjon om status når det gjelder sikkerhetskrav i IKT-anskaffelser, og således bidra til forbedringer i kommunens arbeid på området.

Undersøkelsen har hatt følgende problemstilling:

- Stiller kommunen gode og relevante sikkerhetskrav i anskaffelser på IKT-området?

Problemstillingen er i hovedsak besvart gjennom følgende underproblemstillinger:

- Har de aktuelle virksomhetene vurdert behovet for sikkerhet i systemet som skal anskaffes?
- Har krav til sikkerhet blitt fulgt opp overfor leverandøren fram til systemet er implementert?

## 1.3 Avgrensninger

Undersøkelsen omfatter en revisjon av stilte sikkerhetskrav i IKT-anskaffelser og oppfølgingen av disse kravene fram til driftsettelse. Overholdelse av anskaffelses-regelverket og tiltak iverksatt etter at systemet er satt i drift er ikke revidert. Vi har likevel opplyst om hendelser og prosesser i etterkant av driftsstart i en del tilfeller der dette vurderes som relevant.

Undersøkelsen er gjennomført som en breddeundersøkelse av 15 anskaffelser i 6 virksomheter. Kommunerevisjonen har i hovedsak vurdert prosesskvalitet i denne undersøkelsen. Det innebærer at vi i liten grad har vurdert kvaliteten på det substansielle innholdet i for eksempel risikovurderingene og kravene til informasjonssikkerhet i kravspesifikasjonene, da dette ville kreve forholdsvis inngående kjennskap til hver enkelt anskaffelse og de tilhørende virksomhetsprosesser. Først og fremst betyr dette at Kommunerevisjonen i begrenset grad har undersøkt om alle relevante risikoer har blitt identifisert, og om alle risikoer i tilstrekkelig grad er fulgt opp gjennom sikkerhetskrav. Åpenbare mangler er likevel kommentert der slike har blitt avdekket.

## 1.4 Revisjonskriterier

Revisjonskriteriene er målestokken som ligger til grunn for Kommunerevisjonens vurderinger. Revisjonskriteriene i denne undersøkelsen er blant annet basert på personopplysningsloven, *Instruks for virksomhetsstyring i Oslo kommune* og *Instruks for informasjonssikkerhet i Oslo kommune*. Revisjonskriteriene med grunnlag er nærmere beskrevet i vedlegg 1.

## 1.5 Metodisk tilnærming og gjennomføring

Undersøkelsen har vært rettet mot seks virksomheter og respektive byrådsavdelinger.

Tabell 1 gir en oversikt over anskaffelsene som inngår i revisjonen og hvilken virksomhet som har foretatt anskaffelsene.

***Tabell 1 Oversikt over virksomheter og systemer som inngår i revisjonen***

| Virksomhet | System |
|---|---|
| Utviklings- og kompetanseetaten | HMSREG – Kjernesystem for leverandøroppfølging |
| | Systemstøtte til innkjøpsanalyse |
| | Service Management verktøy |
| Helseetaten | GPS lokaliseringsteknologi |
| | Ledelsesinformasjonsverktøy (LIV) |
| | Kvalitetsstyrings- og internkontrollsystem |
| Bymiljøetaten | Rammeavtale prosjekthotell |
| | Kontrollverktøy parkering |
| | Saksbehandlingsverktøy beboerparkering |
| Barne- og familieetaten | Visma flyt barnevernvakt |
| Utdanningsetaten | Tjeneste for vurdering og kartlegging av læring |
| | Toveis meldingstjeneste for Osloskolen |
| | Fagsystem for Pedagogisk-psykologisk tjeneste (PPT) |
| Bydel Alna | JodaCare |
| | Elektronisk låsesystem og bookingavtale |

Tabell 1 viser at Kommunerevisjonen har undersøkt 15 anskaffelser i 6 virksomheter. For å sikre undersøkelsens relevans ble kun nyere anskaffelser valgt ut. Anskaffelsene ble videre valgt ut for å sikre en bredde av typer systemer, det være seg skytjenester, større fagsystemer og mer begrensede applikasjoner. Kostnadene for systemene spenner seg fra godt under 500 000 kroner for innkjøpet av JodaCare i Bydel Alna til Bymiljøetatens anskaffelse av saksbehandlingsverktøy beboerparkering som hadde en totalverdi på 21 millioner kroner. Virksomhetene ble valgt ut for å dekke variasjon i erfaring med IKT-anskaffelser. Datagrunnlaget i undersøkelsen har i hovedsak bestått av anskaffelsesrelatert dokumentasjon og redegjørelse fra virksomhetene om de valgte IKT-anskaffelsene.

Undersøkelsesperioden har vært styrt av tidslinjen i de valgte anskaffelsene. Vi har som hovedregel valgt anskaffelser som startet opp etter 2015. Imidlertid har mange anskaffelser hatt en lengre historikk, slik at hendelser før 2015 i noen tilfeller er beskrevet. Kommunerevisjonen har valgt å sette et revisjonssluttpunkt til ca. medio mai 2018, det vil si at forhold etter den tid ikke har blitt revidert. Vi har likevel valgt å beskrive enkelte hendelser etter mai 2018 blant annet for å sikre en mer komplett fremstilling av anskaffelsesforløpet.

Metoden og undersøkelsesopplegget er nærmere beskrevet i vedlegg 2.

## 1.6 Rapportens oppbygging

I rapportens kapitler 2 til 7 beskriver vi og vurderer de reviderte virksomhetenes arbeid med informasjonssikkerhet i de valgte anskaffelsene. I kapittel 8 redegjøres det blant annet for virksomhetenes vurdering av modenhet og leveringsevne knyttet til informasjonssikkerhet og informasjonssikkerhetskompetansen til prosjektteamet i anskaffelsen. Kommunerevisjonens konklusjon og anbefalinger presenteres i kapittel 9, og i kapittel 10 oppsummeres og vurderes vesentlige momenter fra uttalelsene til rapporten.

I rapportens vedlegg 1 og 2 følger en nærmere redegjørelse for henholdsvis undersøkelsens revisjonskriterier og metode. Utvalgte begrep som er brukt i rapporten er forklart i vedlegg 3. Uttalelser til rapporten er lagt i vedlegg 4.

# 2. IKT-anskaffelser i Utviklings- og kompetanseetaten

Kommunerevisjonen har gjennomgått tre anskaffelser i Utviklings- og kompetanseetaten:

- Systemstøtte til innkjøpsanalyse – et verktøy for å få kontroll over alle realiserte innkjøp og kostnader knyttet til disse. Verktøyet leveres som en skytjeneste.
- Service management verktøy – et verktøy for å sikre effektiv feilhåndtering, bestillinger og rapportering knyttet til IKT-driftstjenester.
- HMSREG – et system for leverandøroppfølging i utsatte bransjer.

## 2.1 Revisjonskriterier

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
    - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behov for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.
- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

## 2.2 Faktabeskrivelse

### 2.2.1 Systemstøtte til innkjøpsanalyse

***Om systemet***

Formålet med anskaffelsen var å få på plass et tjenestebasert verktøy for å gjøre detaljerte kvantitative innkjøpsanalyser basert på data fra økonomisystemer, bestillingssystemer, fakturaer etc. Verktøyet skulle supplere økonomistyringssystemet Agresso, og det var behov for et ferdig verktøy som enkelt og hurtig kunne implementeres og settes i drift uten å påvirke eller kreve direkte integrasjon mot andre fagsystemer i Oslo kommune.

Anskaffelsen ble gjennomført som en konkurranse med forhandling. Konkurransen ble kunngjort 28.09.2016, og kontrakten ble signert 28.12.2016. Ifølge milepælsplanen i kontrakten skulle verktøyet kunne være kvalitetssikret og tatt i bruk hos kunden 30 dager etter kontraktsignering. Den valgte programvaren skulle leveres som en skyløsning over internett. Ifølge kontrakten var den økonomiske verdien av avtalen ca. 11,5 millioner kroner, inkludert opsjonsår og timebasert bistand.

***Risikovurderinger av informasjonssikkerhet***

Utviklings- og kompetanseetaten hadde utarbeidet en risikovurdering for verktøyet som inkluderte forhold knyttet til informasjonssikkerhet. Risikovurderingen var datert

05.01.2017. Det var etter at kravene var etablert og kontrakten signert. Risikovurderingen identifiserte to hendelser som spesifikt omhandlet informasjonssikkerhet. En av disse omtalte informasjonssikkerhet generelt, uten å være spesifikt knyttet til det konkrete systemet som ble analysert. Den andre hendelsen dreide seg om håndtering av inndata. Sannsynlighet og konsekvens for identifiserte hendelser var etablert i henhold til definerte skalaer, og risikonivå var definert i form av en risikomatrise. Trusler og sårbarheter som kunne påvirke risikonivået var ikke identifisert.

Kontraktstrategien listet opp datakildene som innkjøpsanalysen skulle bygge på og informasjonen som systemet skulle produsere. Det ble her ikke gitt noen vurdering av beskyttelsesbehov og kritikalitet for systemet eller dataene som systemet skulle behandle. Databehandleravtalen som inngikk i konkurransegrunnlaget listet opp typer personopplysninger og taushetsbelagt informasjon som skulle behandles. Her sto det at listen ikke var uttømmende, og at ved tvil om informasjon er sensitiv skulle databehandler ta kontakt med behandlingsansvarlig.

***Krav til informasjonssikkerhet***
Tre informasjonssikkerhetskrav var etablert i etatens kravspesifikasjon, blant annet krav om passordbeskyttet pålogging med mulighet til å styre tilgangsnivå. Kravene inkluderte krav som adresserte den ene hendelsen i risikovurderingen som spesifikt omhandlet informasjonssikkerhet i systemet. Spesielt relevant her var et krav om at leverandøren burde ha et etablert system for behandling av de inndata som mottas fra kunden. Generelt var kravene rettet mot leverandørens rutiner, heller enn av teknisk art. I tillegg stilte databehandleravtalen krav til informasjonssikkerhet, og fastslo dessuten at databehandler skulle følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid hadde bestemt skulle gjelde. Ut over dette var det ikke stilt krav til leverandørens styringssystem for informasjonssikkerhet.

***Bruk av Statens standardavtale***
Kjøpsavtalen SSA-K (kjøpsavtale) var lagt til grunn for anskaffelsen. I Seksjon 1.1. i SSA-K var det gjort et tillegg til standardteksten som understreket at dette ikke var en vanlig kjøpsavtale, men en skytjeneste hvor man betalte for tilgang til en tjeneste.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Det framgikk at leverandørens løsningsforslag for kravene til informasjonssikkerhet var vurdert av Utviklings- og kompetanseetaten.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Etaten kunne ikke dokumentere at det var foretatt sikkerhetstester. Den kunne heller ikke dokumentere andre former for oppfølging av de etablerte sikkerhetskravene fram til implementasjon/driftsettelse. Kravene i kontrakten var i stor grad rettet mot leverandørens rutiner, og altså ikke mot selve systemet.

### 2.2.2 Service management verktøy

***Om systemet***
Systemet skulle være et sentralt verktøy for å sikre effektiv feilhåndtering, bestillinger og rapportering knyttet til IKT-driftstjenester som leveres til Oslo kommunes brukere og virksomheter. Støtte for det eksisterende systemet BOKS gikk ut i januar 2017, og det hadde blitt besluttet å anskaffe et nytt system i stedet for å oppgradere det eksisterende. Løsningen skulle tilrettelegge for at Utviklings- og kompetanseetatens drifts- og forvaltningsleverandører kunne bruke verktøyet til å følge opp saker. I tillegg

skulle det tilrettelegges for at andre virksomheter i Oslo kommune skulle kunne bruke verktøyet som lokal brukerstøtte og/eller håndtering av henvendelser i tilknytning til egne IKT-tjenester. Kontraktstrategien åpnet for at det nye verktøyet kunne leveres enten som en skybasert løsning eller som en løsning i eget IT-miljø. Valget falt til slutt på en skybasert løsning.

Anskaffelsen ble gjennomført som en konkurranse med forhandling og var utlyst 09.02.2016. Kontrakten ble signert 05.10.2016. Løsningen ble satt i drift 22.03.2018. Kontrakten hadde ifølge etaten en antatt verdi på ca. 20 millioner kroner med alle opsjoner og en avtalevarighet på åtte år.

***Risikovurderinger av informasjonssikkerhet***
Det forelå ingen risikoanalyse av informasjonssikkerhet for løsningen som skulle anskaffes. Det var gjennomført en kategorisering av data som skulle behandles i systemet. Disse var inndelt i beskyttelseskategorier på skalaen Lav-Middels-Høy for konfidensialitet, integritet og tilgjengelighet, og videre i informasjonsklassene Åpen/Intern/Intern konfidensielt.

***Krav til informasjonssikkerhet***
Det var stilt flere krav til informasjonssikkerhet i kravspesifikasjonen og databehandleravtalen. Det var blant annet stilt krav til leverandørens styringssystem mv., tilgangsstyring, adskillelse av kundens data fra andre data, overvåkning for å forebygge uønskede hendelser, tilgjengelighet og ivaretakelse av kravene i personvernforordningen.

***Bruk av Statens standardavtale***
Statens standardavtaler SSA-D (driftsavtale) og SSA-T (utviklings- og tilpasningsavtale) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen har mottatt dokumentasjon fra Utviklings- og kompetanseetaten som viser at sikkerhetskrav var inkludert i tildelingskriteriene og at leverandørenes oppfyllelse av kravene var blitt evaluert av etaten. Det fremgikk også fra møtereferat at etaten hadde bedt om ytterligere utdypninger av hvordan noen av kravene ble oppfylt.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Utviklings- og kompetanseetaten hadde ikke gjennomført sikkerhetstester, kun funksjonstester og integrasjonstester. Bortsett fra evalueringen av leverandørens egen besvarelse av hvordan sikkerhetskrav skulle oppfylles, forelå det ikke dokumentasjon av andre former for kontroll av at sikkerhetskravene var oppfylt, for eksempel knyttet til kravet om sikker meldingsutveksling, transport og lagring av data.

### 2.2.3 HMSREG – system for leverandøroppfølging i utsatte bransjer

***Om systemet***
HMSREG skulle være et system for mottak, lagring, kontroll og analyse av mannskapsdata, data om leverandørers og underleverandørers ivaretakelse av økonomiske forpliktelser, samt mulig integrasjon mot offentlige registre og interne systemer i Oslo kommune. På denne måten skulle systemet bidra til å begrense sosial dumping og arbeidslivskriminalitet på alle bygg og anlegg der Oslo kommune var byggherre, inkludert vedlikeholdsoppdrag under rammeavtaler. Konkurransegrunnlaget åpnet for at leverandøren kunne levere systemet som en skyløsning. I så fall måtte leverandøren også stå for drift av denne. Det endelige valget falt på en slik løsning.

Anskaffelsen ble gjennomført som en konkurranse med forhandling og utlyst på Doffin 02.10.2015. Kontraktene ble signert 06.07.2016. Systemet ble ifølge etaten satt i drift 01.02.2017. Ifølge etaten var antatt kontraktsverdi med alle opsjoner estimert til ca 10,1 millioner kroner, med en avtalevarighet på inntil ti år.

***Risikovurderinger av informasjonssikkerhet***
Utviklings- og kompetanseetaten hadde utarbeidet en risikoanalyse som spesifikt adresserte informasjonssikkerhet for systemet. Denne identifiserte ni risikoscenarier. Dokumentet var ikke datert eller oppsatt med en endringslogg. Ifølge etaten var det et dynamisk dokument som var påbegynt før anskaffelsen og ble også benyttet etter at systemet var satt i drift. Status for risikoanalysen på det tidspunkt sikkerhetskravene ble etablert fremgikk derfor ikke.

Analysen identifiserte risikoscenarier og tilordnet konsekvens- og sannsynlighetsverdier for disse. Skala for sannsynlighet var ikke definert i dokumentet. Konsekvensskala var definert, men verdiene som faktisk var tilordnet de identifiserte hendelsene benyttet ikke denne skalaen. Trusler og sårbarheter som kunne påvirke risikonivået var ikke identifisert. Risikonivå var ikke definert i form av risikomatrise eller på annet vis. Tiltak var imidlertid identifisert for alle identifiserte risikoer.

I kontraktstrategien som ble utarbeidet før kravspesifikasjonen, var det også listet opp flere risikoforhold knyttet til informasjonssikkerhet. Disse var blant annet risiko for datamanipulasjon dersom entreprenørene eide registreringsløsningen og risiko for personvernbrudd særlig i tilknytning til utveksling av informasjon med kontrolletatene utenfor kommunen.

Et eget notat om personvern beskrev informasjonstyper som skulle behandles, og inneholdt vurderinger av rettslig grunnlag for behandlingen. Notatet var datert 16.08.2016 og hadde en endringslogg som gikk fra 28.10.2015 til 10.01.2017. I tillegg var det en protokoll for behandling av personopplysninger som ga oversikt over ulike former for behandlinger, samt hvilke personopplysninger som skulle lagres om mannskapet/arbeidstakerne og systembrukerne. Protokollen inneholdt også informasjon om lagring og sletting av dataene, samt tekniske og organisatoriske sikringstiltak.

***Krav til informasjonssikkerhet***
Det var stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Disse omfattet blant annet sikker meldingsutveksling, lagring og transport av data, autentisering og kryptering, og funksjonalitet for å muliggjøre tilgangsbegrensning til data basert på dataenes alder. Det var også stilt krav om bistand til etterlevelse av gjeldende instruks for informasjonssikkerhet, samt at leverandøren skulle ha et styringssystem som ivaretok informasjonssikkerheten i tjenesten. Databehandleravtalen stilte også krav knyttet til informasjonssikkerhet, inkludert krav om sikring av personopplysninger, rutiner for avvikshåndtering og lignende. Det ble her også stilt krav om oppfyllelse av ev. nye informasjonssikkerhetskrav som følge av EUs personvernforordning. Videre var arkitekturprinsippene for Oslo kommunes felles infrastruktur, som har et eget punkt for sikkerhet, tatt med i kontrakten.

De fleste tiltakene for de ni risikoscenariene som ble identifisert i risikovurderingen var ikke systemkrav, men omhandlet etterlevelse av kontrakt, rutiner, leverandøroppfølging og lignende. I de tilfellene Kommunerevisjonen sjekket forelå det sikkerhetskrav for tiltakene identifisert i risikoanalysen.

***Bruk av Statens standardavtale***
SSA-D (driftsavtale) og SSA-T (utviklings- og tilpasningsavtale) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen har mottatt dokumentasjon fra Utviklings- og kompetanseetaten som viser at sikkerhetskrav var inkludert i tildelingskriteriene og at leverandørenes oppfyllelse av kravene var blitt evaluert av etaten. Det fremgikk også at tekniske aspekter ved oppfyllelse av informasjonssikkerhetskrav hadde vært tema i forhandlingene.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Det forelå ikke dokumentasjon for sikkerhetstester eller andre former for kontroll av at sikkerhetskravene var oppfylt fram til driftsettelse, ut over evalueringen av tilbydernes tilbakemeldinger som er omtalt over. Det var gjennomført en system- og integrasjonstest, men denne inkluderte ikke sikkerhetstester.

## 2.3 Kommunerevisjonens vurderinger

***Risikovurderinger av informasjonssikkerhet***
Utviklings- og kompetanseetaten hadde gjennomført risikoanalyser der informasjonssikkerhet var omfattet i to av de tre undersøkte anskaffelsene: *Systemstøtte til innkjøpsanalyse* og *HMSREG*. For førstnevnte var det ikke tilfredsstillende at risikoanalyse kun var gjennomført etter at kravene var etablert og kontrakten var signert. Anskaffelsen manglet dermed et systematisk risikobasert grunnlag for identifisering av sikkerhetsbehov.

Etter Kommunerevisjonens vurdering var det svakheter ved begge risikoanalysene som, uavhengig av tidspunkt for utarbeidelse, kunne ha bidratt til å begrense deres nytte som grunnlag for å etablere sikkerhetskrav. Særlig gjaldt dette *Systemstøtte til innkjøpsanalyse*, hvor kun ett risikoscenario knyttet til informasjonssikkerhet var tilstrekkelig spesifikt til å gi reell støtte for kravutarbeidelse.

I anskaffelsen av *service management verktøy* var det ikke tilfredsstillende at det ikke var gjennomført formelle risikovurderinger i form av en risikoanalyse eller tilsvarende. Det at risikoanalyse manglet ga en risiko for at virksomhetens behov for informasjonssikkerhet i systemet ikke ble dekket i anskaffelsen.

Dataene som systemene skulle behandle var kartlagt og beskyttelsesbehovet vurdert i to av de tre anskaffelsene. For den tredje anskaffelsen var dette mangelfullt.

***Krav til informasjonssikkerhet***
For alle tre anskaffelser var det stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Kommunerevisjonen anser likevel at etaten ikke hadde godt nok grunnlag for utarbeidelsen av kravene, da risikoanalysene som nevnt over, enten ikke var gjennomført eller hadde svakheter som begrenset nytteverdien for kravutarbeidelse.

***Bruk av Statens standardavtale***
I alle tre anskaffelsene var statens standardavtaler benyttet, i tråd med kommunens krav.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
I alle tre anskaffelsene var krav som ble stilt til informasjonssikkerhet i kravspesifikasjonene evaluert av Utviklings- og kompetanseetaten, i tråd med kriteriene i undersøkelsen.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Sikkerhetstester var ikke gjennomført for noen av de tre anskaffelsene. Ut over etatens evalueringer av kravoppfyllelse, som var basert på leverandørens egne tilbakemeldinger, var det heller ikke foretatt andre former for kontroll av at systemene faktisk oppfylte sikkerhetskravene før driftsettelse. Fravær av testing og annen kontroll var en svakhet som innebærer at etaten ikke hadde et tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet i systemene var ivaretatt.

# 3. IKT-anskaffelser i Helseetaten

Kommunerevisjonen har gjennomgått tre anskaffelser i Helseetaten:
- GPS lokaliseringsteknologi
- Ledelsesinformasjonsverktøy (LIV)
- Kvalitetsstyrings- og internkontrollsystem

## 3.1 Revisjonskriterier

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
  - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behov for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.
- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

## 3.2 Faktabeskrivelse

### 3.2.1 GPS lokaliseringsteknologi

***Om systemet***
Behovet i denne anskaffelsen var knyttet til personer som av ulike årsaker hadde behov for å bli lokalisert. Dette omfattet særlig to målgrupper; eldre personer med demens og kognitiv svikt som fortsatt likte å bevege seg ute alene, og personer med funksjonsnedsettelser, spesielt barn og unge. GPS-teknologi hadde før oppstart av anskaffelsen blitt testet ut gjennom et eget prosjekt. Da konkurransegrunnlaget ble utarbeidet var det til sammen ca. 180 aktive GPS-brukere i kommunen, mens forventet antall i løpet av 4 år fra kontraktsinngåelse var ca. 1000 brukere.

Formålet med anskaffelsen var å inngå en ikke-eksklusiv rammeavtale. Både GPS-enheter og tilhørende lokaliseringsapplikasjon for administrasjon, oppfølging og kommunikasjon med enhetene inngikk i løsningen. Fra kundens kravspesifikasjon fremgikk det at lokaliseringsapplikasjonen skulle leveres som en skytjeneste. Helseetaten opplyste at kontraktssummen i kunngjøringen av kontraktstildelingen var oppgitt å være 5 millioner kroner eks. mva.

Anskaffelsen skulle gjennomføres som en konkurranse med forhandling. Den var ikke ferdig gjennomført per mai 2018. Helseetaten har opplyst om at den ved utgangen av mai 2018 var i ferd med å vurdere tilbakemeldinger fra leverandør og revidere tilbud etter gjennomførte forhandlinger, og at kontrakt ble signert 18.06.2018.

***Risikovurderinger av informasjonssikkerhet***
Det forelå ingen risikoanalyse som kunne dannet grunnlag for utforming av sikkerhetskrav. Det var utarbeidet en databehandleravtale som listet opp typer personopplysninger som skulle behandles. Ifølge avtalen var oppramsingen ikke uttømmende, og ved tvil om informasjon var sensitiv skulle databehandler ta kontakt med behandlingsansvarlig. Helseetaten opplyste at aktivitetene for å analysere risiko og informasjonssikkerhet var i oppstart i juli 2018.

***Krav til informasjonssikkerhet***
Kravspesifikasjonen inneholdt krav til informasjonssikkerhet som var spesifikke for det aktuelle systemet, blant annet om soneinndelt administrasjon og tilgangsstyring, sperring av systembrukere for innsyn til enkelte brukere, og tidsbegrenset tilgang for systembrukere. Krav til leverandørens styringssystem for å ivareta informasjons-sikkerheten inngikk også. I tillegg stilte databehandleravtalen krav til informasjonssikkerhet i behandling av personopplysninger.

***Bruk av Statens standardavtale***
Statens standardavtale SSA-K (kjøpsavtalen) var benyttet. Denne er beregnet på kjøp av utstyr og programvare. Som beskrevet over, besto den delen av anskaffelsen som inngår i undersøkelsen av en lokaliseringsapplikasjon som skulle leveres som en skytjeneste.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
På undersøkelsestidspunktet hadde etaten ikke mottatt tilbyderes endelige tilbakemelding på krav til informasjonssikkerhet, og hadde dermed heller ikke evaluert disse.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
På undersøkelsestidspunktet hadde etaten ikke gjennomført kontroll og testing av sikkerhetskrav fram til driftsettelse. Kontrakten viste at test og godkjennelse av kravene i henhold til leverandørens besvarelse, samt sikkerhetsrevisjon av leverandøren, var planlagt. Test av krav med hensyn til informasjonssikkerhet og personvern var også eksplisitt nevnt. Helseetaten hadde også utarbeidet en beskrivelse for akseptansetest som beskrev planlagt testing av informasjonssikkerhetskrav.

### 3.2.2 Ledelsesinformasjonsverktøy (LIV)

***Om systemet***
Anskaffelsen skulle sikre sektoren underlagt daværende Byrådsavdeling for eldre, helse og sosiale tjenester et verktøy for statistikk og analyse som kunne importere og bearbeide informasjon fra de ulike systemene i kommunen. Dette inkluderte blant annet kommunens økonomisystem, Gerica (elektronisk pasientjournal) og GAT (arbeidsplansystem). Dette skulle bidra til raskere og bedre styringsinformasjon, slik at beslutningstakere kunne utnytte tilgjengelige ressurser mer effektivt. Kontrakten var tredelt, med egne deler for 1) programvare, lisenser og opplæring; 2) kjøp av bistandstjenester/konsulenttjenester; 3) vedlikeholdsfasen. Løsningen skulle kjøres i kommunens egen infrastruktur.

Anskaffelsen skulle gjennomføres som en konkurranse med forhandling. Anskaffelsen ble utlyst 26.10.2016. I forkant av dette var det en foregående utlysning som ble avlyst da to av de tre leverandørene som leverte tilbud ble avvist. Kontrakt ble underskrevet i april 2017. Ifølge styringsdokumentet ble løsningen tatt i bruk i januar 2018. Kontraktens totalverdi ble estimert til 6 millioner kroner.

***Risikovurderinger av informasjonssikkerhet***
Helseetaten hadde utarbeidet en risikoanalyse som spesifikt adresserte informasjonssikkerhet for løsningen som skulle anskaffes. Analysen inneholdt blant annet scenarier for tilgang til sensitive data uten tjenstlig behov. Vurderingen var ikke datert, men Helseetaten opplyste at dette var en forenklet risikoanalyse som var gjennomført før driftssetting. Kommunerevisjonen forstår det slik at risikoanalysen forelå etter at sikkerhetskravene i kontrakten var etablert. Helseetaten oppga videre følgende punkter knyttet til ytterligere risikovurderinger:

- Det hadde blitt gjort vurderinger av informasjonssikkerhet i forbindelse med driftsform for anskaffelsen av et annet system for kvalitetsstyring og internkontroll[1], særlig knyttet til hvorvidt en skyløsning skulle brukes. Konklusjonen ble der nei, og på bakgrunn av denne vurderingen ble tilsvarende beslutning tatt for LIV.
- Ved etablering av løsningen ble det gjort en risikovurdering av portåpninger i brannmur for uthenting av data. Risikovurderingen ble gjort av teknisk ressurs hos Oslo kommunes driftsleverandør og ble godkjent av systemeier.
- En mer omfattende risikoanalyse skulle utarbeides. Kommunerevisjonen mottok denne 28.09.2018. Vurderingen var datert 26.07.2018.

Helseetaten hadde i risikoanalysen identifisert og tilordnet sannsynlighets- og konsekvensverdier i henhold til definerte skalaer i de to risikoanalysene. Trusler og sårbarheter som påvirket risikonivået var også identifisert. Risikonivå basert på sannsynlighet og konsekvens var fastsatt i form av en risikomatrise med risikonivåene *høy* (rød), *middels* (gul) og *lav* (grønn).

Det var beskrevet hvilke systemer løsningen skulle hente data fra, og data var kategorisert som henholdsvis sensitive, ikke sensitive og aggregerte. Etaten hadde utarbeidet oversikt over ulike informasjonstyper og klassifisering med hensyn til beskyttelsesbehov i risikoanalysen før driftsettelse.

Databehandleravtalen var laget med utgangspunkt i kommunens mal for dette, og listet også opp typer personopplysninger og taushetsbelagt informasjon som skulle behandles. Avtalen var undertegnet av leverandør og systemeier (Byrådsavdeling for eldre, helse og arbeid) i oktober 2018. Databehandleravtalen gjaldt databehandling leverandøren utførte knyttet til Bistandsavtalen og Vedlikeholdsavtalen. Etaten forklarte at den opprinnelig ikke hadde stilt krav om databehandleravtale, med at valgt leverandør ikke skulle drifte løsningen. Etaten opplyste videre at den arbeidet med å få på plass databehandleravtale med systemleverandører for samtlige av de systemer den forvaltet, der dette manglet.

***Bruk av Statens standardavtale***
Statens standardavtale SSA-V (vedlikeholdsavtale), SSA-K (kjøpsavtale) og SSA-B (bistandsavtale) var benyttet.

***Krav til informasjonssikkerhet***
Krav til informasjonssikkerhet ble stilt i alle de tre avtalene. Kravene var spesifikt tilpasset det aktuelle systemet og omhandlet for eksempel tilgang til sensitive data basert på tjenstlig behov. Det var videre krav om at sensitive personopplysninger skulle håndteres i henhold til kravene i personopplysningsloven og norm for informasjons-sikkerhet (Normen) og krav om at Oslo kommunes arkitekturprinsipper, som inkluderte informasjonssikkerhet, skulle følges. Det ble også stilt krav til informasjonssikkerhet i

[1] Dette er også omfattet av Kommunerevisjonens undersøkelse, og beskrives senere i dette kapitlet.

databehandleravtalen, som blant annet omfattet leverandørens internkontrollsystem for å ivareta informasjonssikkerheten. Databehandleravtalen var imidlertid ikke signert da løsningen ble tatt i bruk.

Ifølge etaten var krav til ikke-akseptert risiko håndtert gjennom krav til tilgangsstyring og krav til at systemet skulle kjøre i sikker sone i Oslo kommunes driftsmiljø, og refererte til vurderingene rundt dette.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Krav til informasjonssikkerhet var evaluert av Helseetaten. Disse ble for en stor del kategorisert som må-krav, hvilket innebar at de skulle besvares med ja/nei. Vurderingen av rettighetsstyring var mer finkornet.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Tester av tilgangsstyring for ulike brukergrupper var inkludert i både testplan, testbeskrivelse og testsluttrapport. I beskrivelsen av hensikten med testplanen ble det ikke sagt noe om sikkerhet eller avdekking av sikkerhetshull/sårbarheter.

I testbeskrivelsen fremgikk det imidlertid at kravet til installering på sikker sone var gjennomgått av Utviklings- og kompetanseetaten gjennom dokumentanalyse, og at det var testet at systemet behandlet data fra kildesystemene korrekt. Kravet om å innfri arkitekturprinsippene var også gjennomgått av etaten. Ut over dette var det ikke gjennomført egne sikkerhetstester.

### 3.2.3 Kvalitetsstyrings- og internkontrollsystem

***Om systemet***
Formålet med anskaffelsen var å få på plass et kvalitetsstyrings- og internkontrollsystem som omfattet kommunens helse- og omsorgstjenester og barnehager. Anskaffelsen var en ny utlysning da avtalen med forrige leverandør ble avsluttet i mai 2017. Anskaffelsen ble gjennomført som en konkurranse med forhandlinger. Veiledende kunngjøring kom i august 2017, mens konkurransen ble kunngjort i januar 2018. Per mai 2018 pågikk det forhandlinger med tilbydere og evaluering av tilbud. Etter planen skulle Sykehjems-etaten som første virksomhet ta i bruk systemet fra februar 2019.

***Risikovurderinger av informasjonssikkerhet***
Det forelå en risikoanalyse som omfatter informasjonssikkerhet. Risikoanalysen var utarbeidet forut for kunngjøring av konkurransen, og resultatene av dette skulle ifølge dokumentet med i anskaffelsens kravspesifikasjon. Scenariene med høyest risiko inkluderte blant annet virusangrep og at driftssenter ble rammet av brann, strømstans mv.

Det fremkom av risikoanalysen at dataene som systemet skulle behandle hadde blitt kartlagt, klassifisert og vurdert med hensyn til beskyttelsesbehov. Kartleggingen viste at mye informasjon ville inneholde taushetsbelagt eller sensitiv informasjon. Dette gjaldt blant annet informasjon knyttet til avviksregistreringer, for eksempel ved tjeneste-tilbudet til pasienter. Av dokumentet fremkom det videre at potensielle trusler og sårbarheter relatert til informasjonssikkerhet hadde blitt identifisert for systemet som skulle anskaffes. Risikoscenarioer hadde også blitt identifisert og det hadde til disse blitt tilordnet sannsynlighet og konsekvens for måloppnåelse og informasjonsverdier.

Skalaene for sannsynlighet og konsekvens var definert. Risikonivå for identifiserte scenarier var blitt fastsatt basert på sannsynlighet og konsekvens, og vurdert opp mot oppsatte risikoakseptansekriterier.

***Krav til informasjonssikkerhet***
I tildelingskriteriene var informasjonssikkerhet vektet til ni prosent. Kravene som lå som vedlegg til utviklings- og tilpasningsavtalen (SSA-T) inneholdt blant annet følgende:

- Leverandøren skulle beskrive sitt styringssystem for informasjonssikkerhet og systemets sikkerhetsarkitektur.
- Systemet skulle kunne driftes på databaser som inneholdt innholdskryptering.
- Leverandøren skal ha en utviklingsmetodikk som fokuserer på teknisk informasjonssikkerhet.

Videre var det krav om et styringssystem hos leverandør som tilsvarte kravene i rammeverket for ISO 27001 (som er et anerkjent rammeverk for styringssystemer for informasjonssikkerhet), krav om etterlevelse av Normen, samt krav om signering av en databehandleravtale.

Etatens kravspesifikasjon inneholdt en rekke sikkerhetskrav som adresserer identifisert risiko. Samtlige av de risikoer Kommunerevisjonen undersøkte nærmere hadde blitt adressert i kravspesifikasjonen.

***Bruk av Statens standardavtale***
SSA-D (driftsavtale) og SSA-T (utviklings- og tilpasningsavtale) var benyttet.

***Status per mai 2018***
Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet og kontroll og testing av sikkerhetskrav fram til driftsettelse var ikke ferdigstilt per mai 2018.

## 3.3 Kommunerevisjonens vurderinger

***Risikovurderinger av informasjonssikkerhet***
Helseetaten hadde gjennomført risikoanalyser før utformingen av sikkerhetskravene i én av de tre undersøkte anskaffelsene, hvor dette gjaldt *kvalitetsstyrings- og internkontrollsystem*. Risikoanalysen var i all hovedsak gjennomført som forutsatt.

I anskaffelsen av *Ledelsesinformasjonsverktøy* var det ikke tilfredsstillende at det ikke var foretatt risikoanalyse før utarbeidelse av kravspesifikasjon, og at det dermed manglet et systematisk risikobasert grunnlag for identifisering av sikkerhetsbehov. Det ble imidlertid gjennomført en risikoanalyse av systemet senere i prosessen, som i hovedsak var gjennomført som forutsatt.

For anskaffelsen *GPS lokaliseringsteknologi* var det ikke tilfredsstillende at det ikke var foretatt en risikoanalyse, og at det dermed manglet et systematisk risikobasert grunnlag for identifisering av sikkerhetsbehov. Dataene som skulle behandles var imidlertid delvis kartlagt i databehandleravtalen. Kommunerevisjonen merker seg at etaten i anskaffelsen hadde planer om en risikoanalyse og sikkerhetsgjennomgang av systemet.

***Krav til informasjonssikkerhet***
I alle tre anskaffelser var det stilt flere sikkerhetskrav. Kommunerevisjonen peker i denne sammenheng på at det for to av systemene manglet risikoanalyser som et

grunnlag for kravene. Dette ga risiko for at virksomhetens behov for informasjons-sikkerhet i systemet ikke ble dekket av sikkerhetskravene.

***Bruk av Statens standardavtale***
I alle tre anskaffelsene var statens standardavtaler benyttet. Standardavtalen som var benyttet i anskaffelsen av *GPS lokaliseringsteknologi* var imidlertid ikke tilpasset det faktum at deler av løsningen skulle leveres som en skytjeneste. Dette kunne gi risiko for at forhold som var typiske for denne type anskaffelser ikke ble tilfredsstillende håndtert.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Av de tre undersøkte anskaffelsene var det kun *ledelsesinformasjonsverktøy (LIV)* som i undersøkelsesperioden hadde kommet så langt at virksomheten hadde mottatt leverandørenes tilbakemeldinger på krav til informasjonssikkerhet. I denne anskaffelsen hadde Helseetaten vurdert leverandørens tilbakemeldinger, i tråd med kriteriene i undersøkelsen.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
For *Ledelsesinformasjonsverktøy (LIV)* hadde Helseetaten gjennomført kontroll av at sikkerhetskrav var ivaretatt i form av vurderinger basert på systemdokumentasjonen, testing av rettighetsstyring og kontroll av behandlingen av inndata i systemet. Ut over dette var det ikke gjennomført egne sikkerhetstester av systemet. Kommunerevisjonen stiller spørsmål om ytterligere kontroll burde vært gjennomført for å få tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet i systemet var ivaretatt. De to øvrige anskaffelsene var ikke driftsatt i løpet av undersøkelsesperioden.

# 4. IKT-anskaffelser i Bymiljøetaten

Kommunerevisjonen har gjennomgått tre anskaffelser i Bymiljøetaten:

- Kontrollverktøy parkering – et automatisert verktøy for parkeringskontroll
- Saksbehandlingssystem beboerparkering – en løsning som skulle støtte bruk av kontrollverktøy for parkering.
- Rammeavtale prosjekthotell – rammeavtale for lagring og prosessering av dokumenter i en skytjeneste.

## 4.1 Revisjonskriterier

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
    - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behov for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.
- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

## 4.2 Faktabeskrivelse

### 4.2.1 Kontrollverktøy parkering

***Om systemet***

Formålet med etatens anskaffelse var å få på plass et kontrollverktøy for parkering. Kontrollverktøyet skulle være påmontert en bil og ta bilder av parkerte kjøretøys kjennemerker og sjekke i databaser om de hadde betalt parkeringsavgift.

Bymiljøetaten organiserte anskaffelsen som en konkurranse med forhandlinger. Ut fra anskaffelsesdokumentasjonen synes det som forhandlingene i hovedsak ble gjennomført i 2016. I april 2017 ble det signert en kontrakt med valgt leverandør. I henhold til framdriftsplanen skulle driftsoppdraget starte i oktober 2017, men ifølge etaten var oppstart september 2018. Dette på grunn av omfattende testing og kalibrering av systemet. Kontraktssum for anskaffelsen var 2,1 mill. kroner eks. mva og årlige driftskostnader.

***Risikovurderinger av informasjonssikkerhet***

Det forelå en risikoanalyse for anskaffelsen som omfattet forhold knyttet til informasjonssikkerhet. Analysen var datert januar 2016, og var dermed gjennomført før utarbeidelse av kravspesifikasjonen. Det ble i analysen identifisert en rekke scenarioer med relevans til informasjonssikkerhet, for eksempel tjenestenektangrep, opplasting av uriktig informasjon og uautorisert tilgang til informasjon i systemet.

Dokumentasjon fra Bymiljøetaten viser at det i desember 2015 ble avholdt møter om blant annet «kartlegging av arbeidsprosesser, informasjon, enighet omkring kritiske/ sårbare informasjonselementment». Etaten hadde utarbeidet et dokument som klassifiserte dataene som skulle behandles og viste disse dataenes vurderte kritikalitet og beskyttelsesbehov.

I risikoanalysen var skala for sannsynlighet og konsekvens blitt etablert og beskrevet. De beskrevne risikoene og risikoscenarioene var blitt tildelt verdier på skalaene for sannsynlighet og konsekvens. Risikonivået for de gjennomgåtte risikoscenariene var blitt fastsatt ved innplassering i en risikomatrise. Matrisen delte risikonivå i grønn, gul og rød risiko. Risikoakseptansekriteriene, det vil si hvilke risikonivåer som krevde avbøtende tiltak og hvilke etaten kunne akseptere, var ikke eksplisitt beskrevet.

***Krav til informasjonssikkerhet***
Det var stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. I kravspesifikasjonen var det blant annet stilt krav om et styringssystem for leverandørs informasjonssikkerhet, støtte til rollebaserte tilgangsløsninger, kryptert datautveksling i kontrollverktøyet og krav til sletting av lagrede data. Flere av kravene gjaldt områder der etaten hadde vurdert at det var risiko.

Vedlagt kravspesifikasjonen var Datatilsynets databehandleravtale. Avtalen skulle inngås som del av kontrakten. I databehandleravtalen identifiseres «kjennemerke til biler» som den personopplysningen som skulle behandles. Avtalen inneholdt en beskrivelse av hvilken behandling av disse dataene som var omfattet av avtalen.

***Bruk av Statens standardavtale***
SSA-T (utviklings- og tilpasningsavtale), SSA-D (driftsavtale) og SSA-V (vedlikeholdsavtale) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen har mottatt dokumentasjon fra Bymiljøetaten på at kravene som ble stilt som tildelingskriterier, og dermed kravene til informasjonssikkerhet, og kvalifikasjonskrav var evaluert av etaten. Tildelingskriteriene var delt opp i *bør* og *må* krav. Eventuelle oppfølgende spørsmål etaten hadde knyttet til leverandørens besvarelse på det enkelte krav, var også blitt dokumentert.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Kommunerevisjonen har mottatt dokumentasjon fra etaten der det er vurdert at alle sikkerhetskravene som var stilt i kravspesifikasjonen var blitt testet og/eller verifisert. Enkelte av sikkerhetskravene dreide seg om rutiner for bruk av systemet.

### 4.2.2 Saksbehandlingsverktøy beboerparkering

***Om systemet***
Formålet med anskaffelsen var å etablere en brukervennlig IKT-løsning for tildeling og saksbehandling av beboerparkering. Løsningen skulle også oppbevare opplysninger som skulle brukes av kontrollverktøy for parkering til å innhente opplysninger om den kontrollerte bilen hadde gyldig beboerparkeringskort.

Anskaffelsen ble foretatt som en konkurranse med forhandlinger, og konkurransen ble kunngjort i Doffin 10.03.2016. Fristen for innlevering av tilbud var 20.06.2016. Kontrakt ble inngått med Cale AS 20.10.2016. Saksbehandlingsverktøyet ble ifølge

etaten tatt i bruk 14.09.2017. Kontraktens totalverdi var ifølge dokumentet *Kunngjøring av kontraktsinngåelse* på ca. 21 millioner kroner.

***Risikovurderinger av informasjonssikkerhet***
Det forelå en risikoanalyse for anskaffelsen som omfattet forhold knyttet til informasjonssikkerhet. Analysen var datert januar 2016, og var gjennomført før utarbeidelse av kravspesifikasjonen. Det ble i analysen identifisert en rekke scenarioer med relevans til informasjonssikkerhet, for eksempel: tjenestenektangrep, at uautoriserte personer får tilgang til systemet, at systemet blir utsatt for skadelig kode i vedlegg (virusangrep) og manglende rutiner for sikkerhetsoppdatering av programvare.

Dokumentasjon fra Bymiljøetaten viser at det i desember 2015, på tilsvarende måte som for kontrollverktøyet for parkering, ble avholdt møter om blant annet «kartlegging av arbeidsprosesser, informasjon, enighet omkring kritiske/ sårbare informasjonselement». Etaten hadde utarbeidet et dokument som klassifiserte dataene som skulle behandles av systemet og viste disse dataenes vurderte kritikalitet og beskyttelsesbehov.

I ovennevnte risikoanalyse var skala for sannsynlighet og konsekvens blitt definert. De beskrevne risikoene og risikoscenarioene var blitt tildelt verdier på skalaene for sannsynlighet og konsekvens. Vurderingen som lå til grunn for disse tildelingene var ikke dokumentert. Risikonivået for de gjennomgåtte risikoscenariene var blitt fastsatt ved innplassering i en risikomatrise. Matrisen delte risikonivå i grønn, gul og rød risiko. Risikoakseptansekriteriene, det vil si hvilke risikonivåer som krevde avbøtende tiltak og hvilke etaten kunne akseptere, var ikke eksplisitt beskrevet.

***Krav til informasjonssikkerhet***
Det var stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Blant annet var det stilt krav til leverandørens styringssystem for informasjonssikkerhet og krav til sikkerhetsrevisjon hos leverandøren. Leverandør skulle også beskrive løsningens utforming for å oppnå tilfredsstillende informasjonssikkerhet. Blant annet var det krav om beskrivelse vedrørende sikring av nettverk og programvare, beskyttelse av programvare og informasjon mot ødeleggelse fra skadelig kode, mekanismer for autorisasjon og tilganger og sikring mot tjenestenektangrep.

Vedlagt kravspesifikasjonen var en databehandleravtale som var basert på Datatilsynets mal for slike avtaler. Denne skulle inngås som del av kontrakten. I databehandleravtalen ble blant annet følgende personopplysninger som skulle behandles identifisert:

- kjennemerke/eierskap til kjøretøy (navn, adresse, e-post og telefonnummer)
- fødselsnummer/DUF-nr.
- status som pendler/student
- hemmelig adresse

***Bruk av Statens standardavtale***
Bymiljøetaten hadde benyttet statens standardavtaler SSA-T (utvikling og tilpasning av programvare), SSA-D (drift) og SSA-V (vedlikehold).

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen har mottatt dokumentasjon fra Bymiljøetaten som viser at sikkerhetskrav var inkludert i tildelingskriteriene og at leverandørenes oppfyllelse av kravene var blitt evaluert av etaten. Tildelingskriteriene var delt opp i bør og må-krav. Eventuelle oppfølgende spørsmål etaten hadde knyttet til leverandørens besvarelse på det enkelte krav, var også blitt dokumentert.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
I kontrakten (SSA-T) ble det lagt opp til at all funksjonalitet og alle integrasjoner skulle testes og godkjennes før systemets driftsstart. Kommunerevisjonen mottok dokumentasjon av testene. Det var ikke spesifisert egne informasjonssikkerhetstester og det fremkom ikke informasjon om funksjonstestene omfattet informasjonssikkerhetskrav.

Bymiljøetaten viste til at sikkerhetsrelevante tester ble utført etter at systemet var tatt i bruk. Utviklings- og kompetanseetaten gjennomførte i perioden 23.10 – 21.11.2017 flere sikkerhetstester i samarbeid med prosjektet og leverandøren av saksbehandlingsverktøyet.

Resultatet av sikkerhetstestene ble oppsummert i en rapport datert 04.12.2017. Konklusjonen i rapporten var at sikkerhetstesten avdekket flere alvorlige avvik og videre at flere av kravene i bestillingens kravdefinisjon ikke var tilfredsstilt.

### 4.2.3 Rammeavtale prosjekthotell

***Om systemet***
Rammeavtalen for prosjekthotell skulle ifølge etaten tilrettelegge for en effektiv samhandling i Bymiljøetatens prosjekter med andre kommunale virksomheter og private samarbeidsparter. Etaten anså at det var behov for en skyløsning for prosjekthotell hvor informasjon kunne utveksles. Konkurransen ble utlyst i begynnelsen av 2017, mens kontraktsignering var i september/oktober 2017. Rammeavtalen hadde ingen fast kontraktsum, men hadde enhetspriser knyttet til månedspris, kurs, bistand mv.

***Risikovurderinger av informasjonssikkerhet i anskaffelsen***
Etaten hadde ikke utarbeidet en risikoanalyse for anskaffelsen. Kommunerevisjonen fikk tilbakemelding fra etaten om at det ikke var krav om slike risikoanalyser i etatens rutiner. Vedrørende datas beskyttelsesbehov var disse ikke blitt systematisk vurdert i anskaffelsen. Etaten ga tilbakemelding om at temaet var diskutert i prosjektet, og de var kommet til at det ikke ville ligge noe sensitive data i løsningen.

***Krav til informasjonssikkerheten***
Det var stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Dette var blant annet krav til styring av tilganger, kryptering av data under overføring, sikring av prosjektdata og personvern, sporbar overvåkning og logging av aktivitet. Det var imidlertid ikke stilt særskilte krav til et styringssystem for informasjonssikkerhet, leverandørs sikkerhetssertifisering eller krav om at en tredjepart foretok kontroll/revisjon av leverandørens sikkerhet.

Det var ikke stilt krav om etablering av en egen databehandleravtale for behandling av eventuelle personopplysninger i skyløsningen.

***Bruk av statens standardavtale***
Bymiljøetaten hadde benyttet statens standardavtale SSA-L (avtale om løpende tjenestekjøp).

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen har mottatt en matrise der leverandørenes løsningsforslag på tildelingskriteriene, herunder ulike sikkerhetskrav, framgikk. Det framkom i all hovedsak med en kortfattet beskrivelse av hva som var etatens evaluering av de stilte sikkerhetskravene.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Det var ikke stilt krav i kontrakt til kontroll eller testing av sikkerhetskrav i systemet før det ble tatt i bruk. Kommunerevisjonen har ikke informasjon om at slike tester eller kontroller ble foretatt.

## 4.3 Kommunerevisjonens vurderinger

***Risikovurderinger av informasjonssikkerhet i anskaffelsen***
Bymiljøetaten hadde gjennomført risikoanalyser i anskaffelsene som gjaldt *kontrollverktøy parkering* og *saksbehandlingsverktøy beboerparkering*, som i all hovedsak var i tråd med undersøkelsens revisjonskriterier.

For anskaffelsen av *prosjekthotell* var det ikke tilfredsstillende at risikoanalyse ikke var gjennomført som ledd i anskaffelsen, og at det dermed manglet et systematisk risikobasert grunnlag for identifisering av sikkerhetsbehov. Etaten hadde heller ikke kartlagt dataene som skulle behandles og vurdert beskyttelsesbehovet for disse.

***Krav til informasjonssikkerheten***
For alle tre anskaffelser var det stilt flere krav til informasjonssikkerhet i kravspesifikasjonen. Flere av kravene i anskaffelsen av *kontrollverktøy parkering* og *saksbehandlingsverktøy beboerparkering* fremsto som relevante på områdene der etaten hadde vurdert at det var risiko. For anskaffelsen av *prosjekthotell* var risikoanalyse ikke gjennomført. Dette ga risiko for at virksomhetens behov for informasjonssikkerhet i systemet ikke ble dekket av sikkerhetskravene.

For *prosjekthotell* stiller Kommunerevisjonen videre spørsmål ved at det ikke var stilt krav om databehandleravtale for behandling av eventuelle personopplysninger, samt om det burde vært krav til leverandørens internkontroll og styringssystem for informasjonssikkerhet, for eksempel gjennom sertifisering.

***Bruk av statens standardavtale***
I alle tre anskaffelser var statens standardavtaler benyttet, i tråd med kommunens krav.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
I alle tre anskaffelsene var kravene til informasjonssikkerhet som ble stilt i kravspesifikasjonen blitt evaluert av Bymiljøetaten, i tråd med undersøkelsens revisjonskriterier.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
For anskaffelsen av *kontrollverktøy beboerparkering* tyder etatens dokumentasjon og redegjørelser på at det før kontraktsstart var testet, eller på annen måte kontrollert, at systemet overholdt stilte informasjonssikkerhetskrav.

For *saksbehandlingsverktøy beboerparkering* viser undersøkelsen at kontrollen av at systemet overholdt stilte informasjonssikkerhetskrav før produksjonsstart var mangelfull. Dette fremgår også fra resultatene fra Utviklings- og kompetanseetatens sikkerhetstester etter systemets driftsstart, som avdekket flere alvorlige sikkerhetssvakheter og at flere av kravene i bestillingens kravdefinisjon ikke var tilfredsstilt.

Kommunerevisjonen stiller spørsmål ved at Bymiljøetaten ikke sørget for sikkerhetstester eller andre former for kontroll av sikkerhetskravene for anskaffelsen av

*prosjekthotell* før driftsstart. Det er derfor risiko for at etaten ikke hadde tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet i systemet var ivaretatt.

# 5. IKT-anskaffelser i Barne- og familieetaten

Kommunerevisjonen har gjennomgått Barne- og familieetatens anskaffelse av et fagsystem for barnevernvakten: *Visma flyt barnevernsvakt*.

## 5.1 Revisjonskriterier

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
  - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behov for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.
- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

## 5.2 Faktabeskrivelse

### 5.2.1 Visma flyt barnevernvakt

***Om systemet***
Systemet var en mobil skybasert løsning som skulle tilgjengeliggjøre fagsystemet for barnevernet via en sikker nettside. Den skulle være et fullverdig fagsystem for barnevernvakten. Tjenesten innebefattet mulighet for digital post og arkiv, og skulle kunne aksesseres via en nettleser på ulike plattformer. Anskaffelsen ble publisert som en frivillig intensjonskunngjøring 03.01.2017, da etaten vurderte at det kun var Visma som kunne levere en løsning tilpasset barnevernets funksjonsområde. Kontrakten ble signert i mars 2017. Ifølge et brev Kommunerevisjonen har mottatt fra etaten, ble installasjon, testing og feilretting utført høsten 2017 og våren 2018. Applikasjonen ble overlevert til Barne- og familieetaten 05.04.2018. Etaten oppga at de planla å ta applikasjonen i aktiv drift i november 2018. Ifølge etaten var den årlige kostnaden i kontrakten på ca. 400.000 kroner. Med tre års varighet på avtalen ble da den totale kontraktssummen ca. 1,2 millioner kroner.

***Risikovurderinger av informasjonssikkerhet***
Det forelå en risikoanalyse som adresserte informasjonssikkerhet for systemet. Denne ble gjennomført etter at sikkerhetskravene var utarbeidet og avtalen inngått, i perioden 28.11.2017 – 23.02.2018, mens selve rapporten ble ferdigstilt 13.04.2018. Risikoanalysen inneholdt konkrete risikoscenarier for systemet, for eksempel scenarier som kunne føre til konfidensialitetsbrudd eller integritetsbrudd for spesifikke informasjonstyper. Disse var tilordnet sannsynlighet og konsekvens for ulike informasjonstyper og for systemet som helhet i henhold til definerte skalaer. Trusler og sårbarheter som påvirket risikonivået var identifisert. Dataene som systemet skulle

behandle var kartlagt og vurdert med hensyn til beskyttelsesbehov. Risikonivå basert på sannsynlighet og konsekvens var definert i form av en risikomatrise.

***Krav til informasjonssikkerhet***
Kravspesifikasjonen inkluderte krav til informasjonssikkerhet, som refererte til ISO 27002[2] og norm for informasjonssikkerhet i helse og omsorgstjenesten (heretter kalt Normen). Det var stilt krav om at leveransen skulle anvende relevante sikkerhetstiltak fra ISO 27002, at leveransen til enhver tid skulle være i henhold til Normen, og at verifisert sjekkliste for å ivareta Normen skulle godkjennes av etaten. Kravene var generelle, og ikke spesifikt utarbeidet for det aktuelle systemet. Men det fantes også enkelte andre krav relatert til informasjonssikkerhet, blant annet om redundans (duplisering av kritiske komponenter og funksjoner), katastrofesikring og tilgjengelighet. I tillegg forelå det også en databehandleravtale som inkluderte krav til informasjonssikkerhet, samt en behovsbeskrivelse fra etaten som inneholdt formuleringer relatert til informasjonssikkerhet, blant annet knyttet til sikker, personlig og sporbar innlogging for hver enkelt bruker, og kryptert oversending av saker til barnevernstjeneste via internett.

***Bruk av Statens standardavtale***
Statens standardavtale SSA-D (driftsavtale) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
På grunn av anskaffelsesformen (direkte anskaffelse) var det ifølge etaten ikke etablert kvalifikasjonskrav eller tildelingskriterier med krav/kriterier til informasjonssikkerhet. I løsningsspesifikasjonen viste leverandør til at løsningen var i tråd med kravene i Normen. Beskrivelsen av sikkerhetsløsninger i løsningsspesifikasjonen var for øvrig lite detaljert. For eksempel sto det at systemet inneholdt muligheter for elektronisk, sikker kommunikasjon, uten at dette ble spesifisert nærmere. Et møtereferat fra 08.09.2017, altså etter at avtalen var inngått, viste at sjekkliste for Normen da hadde blitt gjennomgått. Etaten opplyste at det også var gjennomført flere møter om dette. Sjekklisten inneholdt mer enn 200 punkter av betydning for informasjonssikkerhet. Ifølge referatet fra 08.09.2017 ble det avdekket flere avvik, og det ble bestemt hvem som skulle lukke det enkelte avvik og gitt en tidsfrist for lukking. Kommunerevisjonen mottok en oppfølgingsliste for avvikene som viste at det gjensto ett avvik knyttet til konfigurasjonsendringer.

Ifølge Barne- og familieetaten var det i all hovedsak Normen som var blitt benyttet for å ivareta krav til informasjonssikkerhet, men det ble også gjennomført en test hvor det, for eksempel, ble avdekket avvik knyttet til arkivfunksjonalitet. Dette hadde ført til krav om endring for å ivareta informasjonssikkerhet.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Ifølge Barne- og familieetaten var det utført akseptansetest av systemet, som inneholdt elementer av informasjonssikkerhet. Etaten viste videre til at Utviklings- og kompetanseetaten hadde godkjent integrasjonen av applikasjonen i kommunens felles IKT-miljø (Oslo Felles), og at Utviklings- og kompetanseetaten i den sammenheng hadde gjennomført sikkerhetstester. Utviklings- og kompetanseetaten opplyste imidlertid at godkjenningen besto av overordnete vurderinger, blant annet av at risikoen var vurdert og av konsekvensene for resten av infrastrukturen. Dette inkluderte ikke sikkerhetstesting av systemet.

[2] En anerkjent standard for informasjonssikkerhet, som inneholder anbefalte tiltak for informasjonssikring.

## 5.3 Kommunerevisjonens vurderinger

***Risikovurderinger av informasjonssikkerhet***
Det var ikke tilfredsstillende at etaten ikke gjennomførte risikoanalyse før utarbeidelse av kravspesifikasjonen, og at det dermed manglet et systematisk risikobasert grunnlag for identifisering av sikkerhetsbehov. Ut over at risikoanalysen ble utarbeidet etter etablering av sikkerhetskrav, var den gjennomført som forutsatt.

***Krav til informasjonssikkerhet***
I anskaffelsen var det stilt flere krav til informasjonssikkerhet. Manglende risikoanalyse forut for utarbeidelse av kravspesifikasjonen ga risiko for at virksomhetens behov for informasjonssikkerhet i systemet ikke ble dekket av sikkerhetskravene. Etter Kommunerevisjonens vurdering ble denne risikoen redusert av at kravene i hovedsak var basert på veletablerte domenespesifikke og generelle retningslinjer/standarder.

***Bruk av Statens standardavtale***
Statens standardavtaler var benyttet, i tråd med kommunens krav.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Evalueringen av tilbyders tilbakemelding var i all hovedsak gjennomført ved gjennomgang av sjekkliste for Normen. Leverandørens løsningsspesifikasjon var så lite detaljert at den etter Kommunerevisjonens vurdering ikke var egnet som grunnlag for å evaluere de enkelte punktene i sjekklisten. Kommunerevisjonen anser derfor at etatens evaluering av at krav var innfridd i for stor grad baserte seg på leverandørens vurderinger. Dette er særlig sett i lys av det betydelige omfanget av krav som skulle vurderes, uten at leverandør skriftlig hadde beskrevet hvordan sikkerhetskravene var blitt løst.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Det var ikke gjennomført egne tekniske sikkerhetstester, og akseptansetesten omfattet i begrenset grad informasjonssikkerhet. Kommunerevisjonen merker seg at etaten feilaktig hadde antatt at Utviklings- og kompetanseetaten gjennomførte sikkerhetstesting, uten å forsikre seg om at dette ble foretatt. Kommunerevisjonen mener derfor at ytterligere kontroll burde vært gjennomført for å få tilstrekkelig grunnlag til å fastslå om virksomhetens behov for sikkerhet i systemet var ivaretatt.

# 6. IKT-anskaffelser i Utdanningsetaten

Kommunerevisjonen har gjennomgått tre anskaffelser i Utdanningsetaten:

- Toveis meldingstjeneste for Osloskolen – tjeneste for SMS-kommunikasjon, der primærbrukere er skolene, elever og foresatte.
- Saksbehandlingssystem for PPT – et saksbehandlingsverktøy og styringsverktøy for Utdanningsetaten og PPT.
- Tjeneste for vurdering og kartlegging av læring – nettbasert tjeneste som samler og presenterer resultater og data fra prøver og kartlegginger.

## 6.1 Revisjonskriterier

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
    - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behov for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.
- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

## 6.2 Faktabeskrivelse

### 6.2.1 Toveis meldingstjeneste for Osloskolen

***Om systemet***

Formålet med anskaffelsen var å fornye eller erstatte etatens toveis meldingstjeneste for SMS-kommunikasjon, da foreliggende avtale utløp. Primærbrukere av tjenestene var skolene, elever og foresatte. Utdanningsetaten opplyser at den hadde besluttet å videreutvikle dagens meldingsverktøy i etatens IKT-plattform, og SMS-tjenesten *toveis meldingstjeneste* måtte kunne integreres med denne, i tillegg til at det kunne være behov for integrasjon mot enkelte andre systemer og eksterne tjenesteleverandører. Ifølge avtalen var den økonomiske verdien av avtalen avhengig av antall SMS-meldinger skolene sendte i løsningen.

Konkurransegrunnlaget for anskaffelsen var datert 01.12.2017. Avtalen med Teletopia Interactive AS ble signert og startet opp i april 2018. Systemet som ble anskaffet var fra samme leverandør og det samme systemet som allerede var i bruk i etaten.

***Risikovurderinger av informasjonssikkerhet***

Det ble ikke utarbeidet risikoanalyse forut for kravspesifikasjonen. Etaten oppga at den ikke kunne se at det var spesifikke formkrav til risikovurdering av informasjonssikring i forkant av anskaffelsene, og at hensiktsmessig sikring ble bredt diskutert i møter og

diskusjoner for å få satt relevante krav til tjenestene. Dette gjaldt alle de tre anskaffelse omfattet av undersøkelsen. For *toveis meldingstjeneste for Osloskolen* opplyste etaten at sikkerhetskravene som ble stilt i anskaffelsen var identiske med kravene til øvrige nettbaserte tjenester som er anskaffet i Utdanningsetaten, herunder at det var stilt krav om ivaretakelse av personvern. Kommunerevisjonen har ikke sett at det forelå dokumentasjon av vurderinger av om kravene dekket virksomhetens behov i denne anskaffelsen.

Når det gjaldt spørsmålet om kartlegging av data og vurdering av beskyttelsesbehov, framgikk det av avtalen at systemet skulle behandle personopplysninger. Videre listet inngått databehandleravtale opp ulike typer personopplysninger (herunder sensitive personopplysninger) og taushetsbelagte opplysninger som skulle behandles. Etaten hadde ikke dokumentert eventuelle vurderinger av systemets kritikalitet.

***Krav til informasjonssikkerhet***
I konkurransegrunnlaget ble det stilt krav til informasjonssikkerheten i systemet, blant annet til tilgjengelighet, at brukerdata ikke skulle gå tapt ved driftshendelser, etterlevelse av personopplysningslov og at leverandøren skulle beskrive sin tilnærming til dette kravet. I tillegg inneholdt databehandleravtalen flere krav til informasjonssikkerhet, som at det skulle etableres funksjonalitet som hindret uautorisert tilgang til systemer og informasjon, og krav til tilgangsstyring basert på tjenstlig behov og logging av aktivitet i leverandørens behandling av etatens data

***Bruk av Statens standardavtale***
Statens standardavtale SSA-L (løpende tjenestekjøp) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen mottok dokumentasjon som viser til at etaten hadde vurdert oppfyllelse av de obligatoriske kravene (skal-kravene) i anskaffelsen. De fleste av kravene knyttet til informasjonssikkerhet var i denne kategorien. Det forelå ikke dokumentasjon som viste at bør-kravene var evaluert. Dette gjaldt for eksempel krav om sikring av at brukerdata ikke ble borte på grunn av driftshendelser.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Det framgikk av avtalen at det skulle gjøres akseptansetest etter kontraktsinngåelse. Utdanningsetaten hadde ikke utført tester eller annen kontroll av stilte sikkerhetskrav. Etaten opplyste at tjenesten var identisk med forrige meldingssystem, og viste til at de ville gjennomført sikkerhetstester dersom en annen leverandør var blitt valgt. Etaten kunne ikke vise til dokumenterte sikkerhetstester av forrige meldingssystem.

### 6.2.2 Fagsystem for Pedagogisk-psykologisk tjeneste (PPT)

***Om systemet***
Systemet skulle erstatte tidligere fagsystem for PPT og være et saksbehandlings- og styringsverktøy for Utdanningsetaten sentralt og for PPT internt. Systemet skulle i tillegg kvalitetssikre og dokumentere PPTs produktivitet og produksjon.

Anskaffelsen ble publisert i Doffin i april 2016 og gjennomført som en konkurranse med forhandling. Kontrakten ble underskrevet januar 2017, og løsningen ble ifølge etaten driftsatt i august 2018. Ifølge etaten var kontraktsverdien omlag 13–15 millioner kroner.

***Risikovurderinger av informasjonssikkerhet***
Utdanningsetaten hadde ikke utarbeidet en risikoanalyse forut for etablering av sikkerhetskrav til løsningen. Etaten mente den hadde tilstrekkelig kunnskap om PPTs behov og kritikalitet til å stille relevante sikkerhetskrav i kravspesifikasjonen, uten at dette var avhengig av en risikoanalyse i forkant. Den pekte i den sammenheng på at etatens to sikkerhetskonsulenter var med i hele prosessen. Etaten viste også til en prosjektrapport og en utredningsrapport fra en tidlig fase i anskaffelsen. Disse inneholdt enkelte overordnede risikorelaterte betraktninger, for eksempel ble det i prosjekt-rapporten anbefalt at «…driften av ny løsning beholdes intern i UDE for å kunne ivareta de strenge kravene til informasjonssikkerhet som et fagsystem for PPT må underlegges på grunn av stort innhold av sensitive personopplysninger.» Videre ble det i utrednings-rapporten sagt at løsningen måtte være et system med høy sikkerhet, at den høyeste risikoen lå i å beholde dagens løsning, og at ytterligere risikovurdering ville bli gjort i forbindelse med en anskaffelse.

Leverandøren hadde utarbeidet en risikoanalyse for løsningen, som ble gjennomgått med representanter for etaten 24.10.2017. På grunn av identifiserte avvik i analysen ble løsningen først godkjent 09.11.2017. Utdanningsetaten hadde kun et utdrag av leverandørens risikoanalyse, og Kommunerevisjonen har dermed ikke hatt mulighet til å sjekke risikoakseptansekriterier, definisjoner av skalaer og lignende.

Med hensyn på kartlegging av data som systemet skulle behandle, ga databehandleravtalen en detaljert opplisting av personopplysninger som kunne bli registrert. Vurderinger av kritikaliteten til løsningen var ikke eksplisitt dokumentert, men det fremgikk likevel fra blant annet anskaffelsesstrategien, prosjektforslaget og utredningsrapporten at løsningen var vesentlig for virksomhetens måloppnåelse.

***Krav til informasjonssikkerhet***
Kravspesifikasjonen inneholdt flere sikkerhetskrav, blant annet knyttet til logging av sensitive data, funksjonalitet for overvåkning for å kunne oppdage og varsle uønskede hendelser, kryptering mellom klient og tjener og to-trinns autentisering. Flere av kravene gjaldt også leverandørens håndtering og praktiske arbeid med informasjonssikkerhet, inkludert kvalitetssystem for dette.

***Bruk av Statens standardavtale***
Statens standardavtale SSA-D (driftstjenester) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Etatens evalueringsmatrise som var beslutningsunderlag for valg av leverandør viste at krav til informasjonssikkerhet hadde blitt evaluert av etaten, både i form av vurderinger av må-krav, og ved karaktersetting for andre krav.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Egne sikkerhetstester var ikke gjennomført. I rapporten fra akseptansetesten ble det sagt at «Teknisk sikkerhetstesting som penetrasjonstesting var ikke mulig å gjennomføre på grunn av tilgangene til miljøene på Kundesiden. Det ble istedenfor gjort en vurdering av ROS-analysen [risikoanalyse] til Leverandør.» Denne risikoanalysen er den samme som er omtalt i beskrivelsen av risikoanalyse av informasjonssikkerhet over. Kontroll og testing av sikkerhetskrav ble i all hovedsak gjennomført gjennom etatens oppfølging av leverandørens risikoanalyse og gjennom akseptansetest. Akseptansetesten omfattet sikkerhetskrav som av virksomheten var vurdert å egne seg for denne form for testing. Dette omfattet for eksempel tilgangsstyring og arkivlogg, hvor testen avdekket avvik. Utdanningsetaten hadde fulgt opp avvik som var avdekket i testene.

### 6.2.3 Tjeneste for vurdering og kartlegging av læring

***Om systemet***
Systemet som ble anskaffet var en skytjeneste som samlet og presenterte resultater og data fra prøver og kartlegginger i grunnskolen. Resultatdata skulle innhentes gjennom uttrekk fra det enkelte fagsystem og fra elektroniske registreringsskjema fra lærerne. Resultatene skulle fremstilles i rapporter som underbygget pedagogisk oppfølging av elevene. Elevresultater skulle kunne presenteres på individ-, klasse-, trinn/skole-, skolegruppe og Oslonivå.

Konkurransegrunnlag for anskaffelsen var datert 25.11.2016, og kontrakt med Rambøll Management Consulting ble signert 07.12.2017. Ifølge Utdanningsetaten var systemet på undersøkelsestidspunktet (oktober 2018) ikke driftsatt, da akseptansetesten ikke var godkjent. Etaten opplyste at dette ikke skyldtes sikkerhetsmessige forhold.

Ifølge avtalen var den økonomiske verdien av avtalen 900 000 kroner i etableringskostnader for systemet og 350 000 kroner i årlige driftskostnader.

***Risikovurderinger av informasjonssikkerhet***
Utdanningsetaten hadde ikke foretatt en dokumentert risikoanalyse av informasjonssikkerhet for løsningen som skulle anskaffes, ut over at det i kontraktstrategien framkom en risiko for brudd på personvernlovgiving. Det ble her pekt på at systemet ville inneholde personopplysninger, var webbasert, og at data kunne komme på avveie. Utdanningsetaten opplyste til Kommunerevisjonen at det var snakk om et standardprodukt, og at det derfor ikke skulle utvikles et nytt system. Dette var en medvirkende årsak til begrenset omfang på risikovurderinger.

Med hensyn på kartlegging av data og vurdering av beskyttelsesbehov, hadde etaten oversikter som beskrev hvilke persondata som skulle behandles i systemet, og det framgikk i kontraktstrategi og konkurransegrunnlag at systemet måtte ivareta krav til behandling av personopplysninger.

***Krav til informasjonssikkerhet***
Kravspesifikasjonen omfattet en rekke overordnede krav til informasjonssikkerhet, herunder til etterlevelse av personopplysningslov, transportkryptering og til at leverandøren jevnlig skulle gjennomføre risikovurdering og nødvendig tiltak for å sikre tilfredsstillende informasjonssikkerhet. Det framgikk også at «Tilgangsstyringen i tjenesten bør være basert på det overordnede prinsippet om at personinformasjon kun er synlig for de brukerne som har et tjenestemessig behov for dette». Videre ble det stilt en rekke krav til informasjonssikkerhet i en midlertidig databehandleravtale signert 21.11.2017. Etaten opplyser at endelig databehandleravtale, basert på Oslo kommunes nye utkast til mal, ville bli underskrevet før oppstart.

***Bruk av Statens standardavtale***
Statens standardavtale SSA-D (kjøp av driftstjeneste) var benyttet.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
Kommunerevisjonen har mottatt et evalueringsdokument der det framgikk at etaten hadde evaluert tilbakemeldingen fra tilbyder på sikkerhetskravene. I løsningsforslaget dokumenterte også leverandøren sin internkontroll gjennom revisorrapport ISAE 3000 type 2 fra PwC.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Det framgikk av avtalen at Utdanningsetaten skulle gjennomføre akseptansetest, og etaten opplyste i juni 2018 om at dette da pågikk. Kommunerevisjonen har mottatt en oversikt som viser at informasjonssikkerhetskravene inngikk i testplan for akseptansetest. Unntak var krav etaten vurderte ikke egnet seg for test, som at leverandøren skulle gjennomføre løpende risikovurdering.

## 6.3 Kommunerevisjonens vurderinger

***Risikovurderinger av informasjonssikkerhet***
Etter Kommunerevisjonens vurdering er det ikke tilfredsstillende at Utdanningsetaten manglet et systematisk risikobasert grunnlag for identifisering av sikkerhetsbehov i alle de tre anskaffelsene. Data som skulle behandles var imidlertid blitt kartlagt som ledd i anskaffelsene. Etaten pekte på forhold som kunne bidra til å forklare manglende risikoanalyser, som for eksempel at de la etatens standard sikkerhetskrav til grunn. Det at risikoanalyser ikke forelå ga likevel risiko for at virksomhetens behov for informasjonssikkerhet i hvert enkelt system ikke ble dekket.

***Krav til informasjonssikkerhet***
I alle tre anskaffelser var det stilt flere sikkerhetskrav. Kommunerevisjonen peker i denne sammenheng på at det manglet risikoanalyser som et grunnlag for kravene. Det at risikoanalyser ikke var blitt gjennomført ga likevel risiko for at virksomhetens behov for informasjonssikkerhet i systemet ikke ble dekket av sikkerhetskravene.

***Bruk av Statens standardavtale***
I alle tre anskaffelsene var statens standardavtaler benyttet, i tråd med kommunens krav.

***Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet***
I to av de tre anskaffelsene var krav som ble stilt til informasjonssikkerhet i kravspesifikasjonene evaluert av Utdanningsetaten, som forutsatt.

I anskaffelsen av *toveis meldingstjeneste for Osloskolen* var det en svakhet at etaten ikke hadde gjennomført en skriftlig evaluering av alle sikkerhetskravene.

***Kontroll og testing av sikkerhetskrav fram til driftsettelse***
Sikkerhetssvakheter vil i mange tilfeller ikke fremkomme ved ordinær drift. Det er derfor en svakhet at Utdanningsetaten ikke hadde testet, eller på annen måte kontrollert, kravene til informasjonssikkerhet i anskaffelsen av *toveis meldingstjeneste for Osloskolen* med den begrunnelse at systemet allerede var i bruk.

For *fagsystem for PPT* var det gjennomført akseptansetest som omfattet de sikkerhetskravene som av etaten var vurdert å egne seg for denne form for testing.

Det hadde det ikke blitt gjennomført egne tekniske sikkerhetstester før driftsettelse. Kommunerevisjonen stiller spørsmål om etaten uten slik testing hadde tilstrekkelig grunnlag for å vurdere om sikkerheten i systemet var i tråd med etatens behov.

I anskaffelsen av *tjeneste for vurdering og kartlegging av læring* var det i undersøkelsesperioden gjennomført akseptansetest som omfattet de sikkerhetskravene som av etaten var vurdert å egne seg for denne form for testing. Tekniske sikkerhetstester var ikke gjennomført i undersøkelsesperioden. Systemet var per mai 2018 i en testfase, og var per oktober 2018 ikke driftsatt.

# 7. IKT-anskaffelser i Bydel Alna

Kommunerevisjonen valgte ut to mindre IKT-anskaffelser i Bydel Alna for revisjon. Anskaffelsene var kjøp av en kommunikasjonsløsning mellom pårørende og helsepersonell (JodaCare) og kjøp av et system for elektroniske låser (ARX). Booking av lokaler lå inne som en tilleggsopsjon i kjøpet.

## 7.1 Revisjonskriterier

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
  - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behov for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.
- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

## 7.2 JodaCare

***Om systemet***
JodaCare var ifølge leverandør en løsning (App) som skulle gi bedre kommunikasjon og samarbeid mellom pårørende og helsepersonell. Leverandør oppga at systemet skulle benyttes til informasjon om daglige gjøremål, og at det ikke skulle legges sensitiv informasjon i systemet. Systemet omfattet funksjonalitet for beskjeder, bilder, kalender og personlig profil ifølge leverandørens hjemmeside.

Ifølge bydelen ble JodaCare tatt i bruk som del av et prosjekt i oktober 2016 ved Haugerud og Furuset seniorsenter. Ifølge bydelen var systemet kun tatt i bruk ved innhentet samtykkeerklæring med bruker og pårørende, og det hadde kun vært aktivt i bruk på Furuset seniorsenter da interessen på Haugerud seniorsenter hadde vært for lav. Basert på mottatt kontrakt synes kostnadene for systemet å være 125 kroner i måneden per tjenestemottaker.

***Bydelens vurdering av behov for sikkerhet i systemet***
Det foreligger ikke dokumentasjon på at behovet for sikkerhet i systemet ble vurdert gjennom egne risikovurderinger, kartlegging av informasjonsverdier eller tilsvarende da systemet ble kjøpt inn i 2016. Kjøpet var, ifølge bydelen, foretatt av tjenestestedet i bydelen, uten at bydelens IKT-ressurs var involvert og informert.

På spørsmål om sikkerhet i systemet viste bydelen i e-post av juni 2018 til at JodaCare ville benytte innlogging med BankID fra sommeren 2018. Bydelen viste videre til en e-post fra leverandøren til bydelen av november 2017 der det ble presentert en del retningslinjer for hva brukere kunne registrere/dele i JodaCare. Formålet med

retningslinjene synes å være at sensitiv informasjon ikke skulle legges inn i systemet. For eksempel kunne det gis informasjon om «daglige gjøremål». Bydelen opplyste også at seniorsentrene hadde presisert at det ble innhentet samtykkeerklæring i bruk av JodaCare. I en redegjørelse fra bydelen til Kommunerevisjonen ble det vist til at «Systemet har gått igjennom flere ROS-analyser i Bærum og Trondheim».

***Krav til og oppfølging av sikkerhet i systemet***
Kommunerevisjonen mottok en kontrakt som ifølge bydelen ble signert 11.06.2018 og en databehandleravtale datert 20.02.2018. Kontrakten inneholdt ikke noen omtale av forhold relatert til informasjonssikkerhet. Databehandleravtalen regulerte databehandlers behandling av personopplysninger. Bydelen har ikke kunne fremskaffe andre avtaledokumenter som regulerer/omtaler behandling av informasjonssikkerhet i systemet eller på annen måte har sannsynliggjort at det var blitt stilt krav til informasjonssikkerhet i systemet frem til systemet ble satt i drift i bydelen.

## 7.3 Elektronisk låsesystem og bookingavtale

***Om systemet***
Bydel Alna og Deichman bibliotek inngikk en avtale i desember 2015 med en leverandør om etablering av et elektronisk låsesystem ved Furuset bibliotek og aktivitetshus. Avtalen omfattet som en opsjon et selvbetjent bookingsystem som skulle leveres av en underleverandør. Av kontrakten fremgikk det at avtalen var del av et pilotprosjekt for å tilrettelegge for at frivillige kunne benytte bydelens lokaler til åpne arrangementer. Eksterne kunne med systemet reservere rom og få tilgang til rom/fasiliteter gjennom en elektronisk nøkkel. Det var også et krav til systemet at det kunne tas betaling eller reserveres depositum fra bankkort. I januar 2016 ble det etablert en avtale om installasjon og drift av samme system i Lindeberglokalet, og i oktober 2017 ble en tilsvarende avtale inngått ved Haugerud aktivitetshus. Bookingavtalen var ifølge bydelen ikke i bruk på Haugerud. Samlet kontraktsum for avtalene syntes å være mellom 300 000 og 400 000 kroner.

***Bydelens vurdering av behov for sikkerhet i systemet***
Det foreligger ikke dokumentasjon på at behovet for sikkerhet i systemet ble vurdert gjennom egne risikovurderinger, kartlegging av informasjonsverdier eller tilsvarende da systemet ble kjøpt inn. Ifølge bydelen var kjøpet foretatt av tjenestestedet i bydelen, uten at bydelens IKT-ressurs var involvert og informert.

***Statens standardavtaler***
Bydelen hadde benyttet statens standardavtale om konsulenttjenester (SSA-O). For drift eller såkalt hosting av systemet var avtalen basert på leverandørens tilbudsbeskrivelse.

***Krav til og oppfølging av sikkerhet i systemet***
I henhold til bilag til kontrakt av desember 2015 skulle systemet ha en støtte for rolledeling. Foreslåtte roller var administrator/bookingansvarlig, førsteprioritetsbruker og sluttbruker / eksterne aktører. I bilag til kontrakten fremkom det at systemet skulle feilrettes og videreutvikles etter at systemet var installert. Kommunerevisjonen har ikke mottatt ytterligere dokumentasjon om dette.

Bydelen har ikke kunnet oversende dokumentasjon eller på annen måte sannsynliggjort at det var blitt stilt krav til informasjonssikkerhet i forbindelse med at systemet ble satt i drift ved de aktuelle lokasjonene i bydelen.

## 7.4 Kommunerevisjonens vurderinger

Begge de undersøkte systemene hadde et relativt begrenset virkeområde, noe som kan ha følger for forventningene til omfanget av risikovurderinger og kontroller av sikkerhetskrav. Samtidig var det risiko for at systemene kunne inneholde informasjon med beskyttelsesbehov.

Det var etter Kommunerevisjonens vurdering vesentlige mangler og svakheter ved sikkerhetskravene i bydelens anskaffelser. Svakheten innebærer at bydelen ikke hadde sikret seg at de to systemene hadde nødvendig informasjonssikkerhet ved innkjøpet av systemene. Vurderingen bygger på at:

- det ikke forelå noen risikoanalyse eller kartlegging av informasjonsverdier forut for anskaffelse og driftsetting av de to systemene,
- sikkerhetskrav manglet for ett av systemene, og
- det ikke forelå dokumenterte sikkerhetstester eller andre former for kontroll av at sikkerhetskravene var oppfylt før driftsetting av systemene.

Bydelens avtale om et elektronisk låse- og bookingsystem inneholdt enkelte informasjonssikkerhetskrav. Manglende risikovurderinger og dokumenterte kontroller gjør at bydelen likevel ikke hadde sikret seg at systemet hadde tilstrekkelig sikkerhet, særlig med tanke på at systemet skulle kunne håndtere betaling med bankkort.

Det var en vesentlig svakhet ved anskaffelsen av JodaCare at krav til informasjons-sikkerhet ikke inngikk i avtalen som ble inngått da systemet ble anskaffet. Leverandørens senere presiseringer av behov for driftsrutiner og sikkerhet ved innlogging viser dette tydelig.

Begge avtaler var i utgangspunktet under terskelverdien for når statens standardavtaler skulle benyttes.

Manglene og svakhetene påpekt ovenfor gir risiko for at data kommer på avveie, går tapt eller misbrukes. Når det gjelder JodaCare, kan dette for eksempel innebære at uvedkommende får tilgang til sensitive personopplysninger.

# 8. Beskrivelse av ulike forhold i anskaffelsene

I dette kapitlet belyses virksomhetenes praksis på ulike områder av betydning for anskaffelsene. Kapittelet beskriver virksomhetenes tilbakemelding på spørsmål fra Kommunerevisjonen hva gjelder

- deres vurdering av leverandørens modenhet og leveringsevne knyttet til informasjonssikkerhet
- informasjonssikkerhetskompetanse i prosjektteamet som deltok i anskaffelsen
- regulering av eiendomsretten til data og systemer i kontraktene

***Leverandørens modenhet og leveringsevne knyttet til informasjonssikkerhet***

Tabell 2 oppsummerer virksomhetenes grunnlag for vurderinger av leverandørens modenhet og leveringsevne knyttet til informasjonssikkerhet. Oppsummeringen er basert på virksomhetenes redegjørelse på spørsmål fra Kommunerevisjonen samt informasjon fra anskaffelsesdokumentasjonen.

***Tabell 2 Leverandørens modenhet og leveringsevne knyttet til informasjonssikkerhet***

| Virksomhet | System | *Var leverandørens modenhet og leveringsevne knyttet til informasjonssikkerhet vurdert?* |
|---|---|---|
| Utviklings- og kompetanse-etaten | HMSREG – system for leverandøroppfølging i utsatte bransjer | Krav i kravspesifikasjonen om et styringssystem som ivaretok informasjonssikkerhet i tjenesten |
| | Systemstøtte til innkjøpsanalyse | (Det var stilt sikkerhetskrav i kravspesifikasjonen) |
| | Service Management verktøy | Kvalifiseringskrav om kvalitetssikringssystem som omfattet informasjonssikkerhet og personvern |
| Bymiljø-etaten | Rammeavtale prosjekthotell | Etaten viste til at aktuelle systemer var hyllevare og at etaten kjente markedet godt. |
| | Kontrollverktøy parkering | (Det var stilt sikkerhetskrav i kravspesifikasjonen) |
| | Saksbehandlingsverktøy beboerparkering | Etaten viste til at dette var vurdert i flere workshops knyttet til anskaffelsen |
| Utdannings-etaten | Tjeneste for vurdering og kartlegging av læring | Dokumentert internkontroll gjennom revisorrapport |
| | Toveis meldingstjeneste for Osloskolen | Ingen vurdering, etaten viste til at leverandør og system var uendret etter anskaffelsen |
| | Fagsystem for PPT | Kvalifiseringskrav om dokumentasjon av informasjonssikkerhetserfaring og internkontroll |
| Helseetaten | GPS lokaliseringsteknologi | (Det var stilt sikkerhetskrav i kravspesifikasjonen) |
| | Ledelsesinformasjons-verktøy (LIV) | Kvalifiseringskrav om at aspekter ved leverandørens informasjonssikkerhetserfaring skulle dokumenteres. |
| | Kvalitetsstyrings- og internkontrollsystem | Leverandørs styringssystem for informasjonssikkerhet var ISO 27001-sertifisert. Kartlegging av sider ved aktuelle leverandørers modenhet/kompetanse på informasjons-sikkerhet i en tidlig fase i anskaffelsen. |
| Barne- og familie-etaten | Visma flyt barnevernvakt | Leverandørs styringssystem for informasjonssikkerhet var ISO 27001-sertifisert |
| Bydel Alna | JodaCare | Ingen vurdering |
| | Elektronisk låsesystem og bookingavtale | Ingen vurdering |

Note: Tabellen er utarbeidet på bakgrunn av virksomhetenes tilbakemelding på spørsmål fra Kommunerevisjonen. I tillegg er det lagt inn supplerende informasjon fra kvalifikasjonskravene og kravspesifikasjonen.

Tabell 2 viser at virksomhetene som hovedregel ikke hadde stilt eksplisitte krav til leverandørens modenhet og leveringsevne på informasjonssikkerhet i kvalifiseringen. Unntaket her var knyttet til tre av anskaffelsene i regi av henholdsvis Helseetaten, Utviklings- og kompetanseetaten og Utdanningsetaten. I ytterligere én av Helseetatens anskaffelser var det gjort vurderinger i en tidlig fase av anskaffelsen.

Som det fremgår av kapittel 2-7 var det i de fleste anskaffelsene i kravspesifikasjonen stilt sikkerhetskrav som var blitt evaluert. Slik evaluering er kun tatt inn i tabellen der dette er det eneste meldte eller aktuelle tiltaket.

***Informasjonssikkerhetskompetanse i anskaffelsesprosjektet***
Tabell 3 gir en oversikt over hva virksomhetene oppga om sin bruk av særskilt informasjonssikkerhetskompetanse i de ulike anskaffelsesprosjektene.

***Tabell 3 Informasjonssikkerhetskompetanse i anskaffelsesprosjektet***

| **Virksomhet** | **System** | ***Har personer med særskilt informasjonssikkerhets-kompetanse deltatt i anskaffelsesprosjektet?*** |
|---|---|---|
| Utviklings- og kompetanseetaten | HMSREG – system for leverandøroppfølging i utsatte bransjer | Ja, blant annet i arbeidet med risikovurderinger. |
| | Systemstøtte til innkjøpsanalyse | Nei. Jurist deltok i utarbeidelsen av databehandleravtalen. |
| | Service Management verktøy | Ja. Avgitt en egen til ressurs prosjektet.* |
| Bymiljøetaten | Rammeavtale prosjekthotell | Nei |
| | Kontrollverktøy parkering | Ja, i flere faser av anskaffelsen. |
| | Saksbehandlingsverktøy beboerparkering | Ja, i flere faser av anskaffelsen. |
| Utdanningsetaten | Tjeneste for vurdering og kartlegging av læring | Ja, i en tidlig fase av prosjektet og i utforming av sikkerhetskrav. |
| | Toveis meldingstjeneste for Osloskolen | Nei |
| | Fagsystem for PPT | Ja, i flere faser av anskaffelsen. |
| Helseetaten | GPS lokaliseringsteknologi | Ja, i flere faser av anskaffelsen. |
| | Ledelsesinformasjonsverktøy (LIV) | Ja, i flere faser av anskaffelsen. |
| | Kvalitetsstyrings- og internkontrollsystem | Ja, i flere faser av anskaffelsen. |
| Barne- og familie-etaten | Visma flyt barnevernvakt | Ja, i flere faser av anskaffelsen. |
| Bydel Alna | JodaCare | Nei |
| | Elektronisk låsesystem og bookingavtale | Nei |

Note: Tabellen er basert på redegjørelser og/eller dokumentasjon fra virksomhetene om informasjonssikkerhetskompetansen som var benyttet i anskaffelsen. Vi har ikke etterspurt sertifiseringer, vitnemål eller annet. *Etaten opplyste i uttalelse til rapport at det var avgitt en egen informasjonssikkerhetsressurs i 20 prosent gjennom anskaffelsesprosjektet.

Tabell 3 viser at det, ifølge virksomhetene, var blitt benyttet personell med særskilt informasjonssikkerhetskompetanse i de fleste anskaffelsene.

Kommunerevisjonen har ikke kartlagt hvilken formell informasjonssikkerhets-kompetanse de aktuelle personene hadde. Det er videre ikke i detalj blitt kartlagt hvilke anskaffelsesfaser personene var involvert i og omfanget av deltagelse i ulike faser.

***Eiendomsrett til data og systemer***
Bruk av relevant standardavtale fra staten vil normalt sikre en avtale som tydelig regulerer eiendomsrett/råderett til data og systemer. Med unntak av de to anskaffelsene i Bydel Alna, var det i alle anskaffelsene utarbeidet kontrakter som regulerte eiendomsrett og råderett til data og systemer i den grad det var aktuelt. For eksempel er det i utgangspunktet ikke aktuelt særskilt å regulere eiendomsretten til systemet når en skytjeneste skal anskaffes, fordi man da kjøper en tjeneste, og ikke et system.

I Utviklings- og kompetanseetatens anskaffelse av *systemstøtte til innkjøpsanalyse* ble det benyttet en standard kjøpskontrakt som ikke hensyntok at tjenesten som ble kjøpt inn var en skytjeneste. Det var utarbeidet en databehandleravtale som fastslo at databehandler ikke hadde råderett over personopplysningene og taushetsbelagt informasjon. Leverandørens råderett over data som verken var personopplysninger eller taushetsbelagte var, etter det Kommunerevisjonen kan se, ikke regulert.

# 9. Kommunerevisjonens konklusjoner og anbefalinger

Kommunerevisjonen har undersøkt om kommunen stiller gode og relevante sikkerhetskrav i anskaffelser på IKT-området. Dette er gjort gjennom å undersøke om utvalgte virksomheter hadde vurdert behovet for sikkerhet i IT-systemene som var blitt anskaffet, og om krav til sikkerhet ble fulgt opp ovenfor leverandørene fram til systemene ble implementert. Undersøkelsen er gjennomført som en breddeundersøkelse av 15 anskaffelser i 6 virksomheter: Utviklings- og kompetanseetaten, Helseetaten, Bymiljøetaten, Barne- og familieetaten, Utdanningsetaten og Bydel Alna. Kommunerevisjonen har i hovedsak vurdert prosesskvalitet.

Kommunerevisjonen har videre beskrevet virksomhetenes vurdering av leverandørenes modenhet og leveringsevne knyttet til informasjonssikkerhet og virksomhetenes kompetanse på informasjonssikkerhet i anskaffelsesprosjektene.

## 9.1 Om informasjonssikkerhetskompetanse og leverandørenes modenhet

De undersøkte virksomhetene oppga i hovedsak å vurdere modenhet og leveringsevne når det gjelder informasjonssikkerhet ved evaluering av leverandørenes tilbud. Kun i et fåtall tilfeller var det i kvalifikasjonsgrunnlaget stilt spesifikke krav til modenhet og leveringsevne i tilknytning til informasjonssikkerhet. I tre av anskaffelsene ble ikke modenhet og leveringsevne knyttet til informasjonssikkerhet vurdert. Dette gjaldt anskaffelser foretatt av Bydel Alna og Utdanningsetaten.

I fem av de 15 anskaffelsene ble det ifølge virksomhetene ikke benyttet særskilt informasjonssikkerhetskompetanse. I de resterende anskaffelsene ble det vist til at prosjektet hadde hatt tilknyttet personell med informasjonssikkerhetskompetanse i flere faser i anskaffelsen. Kommunerevisjonen har ikke kartlagt hvilke anskaffelsesfaser disse personene var involvert i og omfanget av deltagelse i ulike faser.

Bruk av relevant standardavtale fra staten vil normalt sikre en avtale som tydelig regulerer eiendomsrett til data og systemer. Med unntak av de to anskaffelsene i Bydel Alna, var det i alle anskaffelsene utarbeidet kontrakter som regulerte eiendomsretten til data og systemer. I Utviklings- og kompetanseetatens anskaffelse av systemstøtte til innkjøpsanalyse ble det imidlertid benyttet en standard kjøpskontrakt som ikke hensyntok at tjenesten som ble kjøpt inn var en skytjeneste.

## 9.2 Konklusjoner

Undersøkelsen viser at virksomhetene for de fleste anskaffelsene hadde stilt informasjonssikkerhetskrav til systemene som ble anskaffet. Imidlertid hadde virksomhetene i et fåtall av de undersøkte anskaffelsene gjennomført risikovurderinger av informasjonssikkerhet som kunne gi grunnlag for sikkerhetskravene. Etter Kommunerevisjonens vurdering innebærer dette at flere av de undersøkte virksomhetene ikke hadde sørget for tilfredsstillende prosesser som grunnlag for gode og relevante sikkerhetskrav. I tillegg var det svært begrenset sikkerhetstesting før systemene ble satt i drift. Det gir risiko for at informasjonssikkerheten ikke var ivaretatt før systemet ble tatt i bruk. Det var også enkelte andre svakheter.

Samlet gir identifiserte mangler og svakheter risiko for at sikkerheten i de anskaffede systemene ikke var 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 tilgjengelige ved

behov. Flere av de undersøkte anskaffelsene var av systemer som behandlet store mengder sensitiv informasjon, for eksempel barnevernsaker og helseopplysninger.

Følgende oppsummerer de sentrale funnene i undersøkelsen:

- I de fleste tilfellene var det ikke gjennomført risikoanalyser i forkant av kravspesifikasjon. I enkelte tilfeller var det heller ikke foretatt kartlegging og vurdering av beskyttelsesbehov til de dataene som skulle behandles.
- Det varierte om gjennomførte risikovurderinger var tilfredsstillende utført.
- I de fleste anskaffelsene var det foretatt tilfredsstillende evalueringer av leverandørens tilbakemeldinger på sikkerhetskrav. I enkelte tilfeller var slike evalueringer mangelfulle eller ikke gjennomført. Dette var tilfelle i anskaffelser foretatt av Barne- og familieetaten og Utdanningsetaten.
- I de aller fleste anskaffelsene var det gjennomført kontroll av at sikkerhetskrav var overholdt, basert på gjennomgang av dokumentasjon eller vurderinger fra leverandøren. Det var imidlertid i liten grad gjennomført egne sikkerhetstester.
- Bydel Alna hadde ikke gjennomført nødvendige prosesser for å sikre at IT-systemene hadde sikkerhet i tråd med bydelens behov.

## 9.3 Anbefalinger

Anbefalinger som gjelder alle de reviderte virksomhetene:

- Virksomhetene bør vurdere tiltak som kan gi større trygghet for at systemer som anskaffes har et sikkerhetsnivå i tråd med virksomhetens behov. Særlig bør det sikres at virksomheten har
  - sørget for tilstrekkelige risikoanalyser som grunnlag for informasjonssikkerhetskrav i kravspesifikasjoner, og
  - gjennomført tilstrekkelig kontroll av at systemer som anskaffes ivaretar sikkerhetsbehovene, herunder at det er gjennomført egne sikkerhetstester ved vurdert behov.

Anbefalinger som gjelder enkelte virksomheter:

- Barne- og familieetaten og Utdanningsetaten bør sørge for en tilfredsstillende evaluering av leverandørers tilbakemelding på sikkerhetskrav i kravspesifikasjoner.
- Bydel Alna bør sørge for tilstrekkelig kontroll med anskaffelsesprosessene slik at det stilles nødvendige risikobaserte krav til informasjonssikkerhet, at kravene evalueres på en tilfredsstillende måte og at det gjennomføres nødvendige kontroller og testing av sikkerhetskrav før IT-systemer settes i drift.

# 10. Uttalelser til rapporten og Kommunerevisjonens vurderinger

Rapporten ble 20.11.2018 sendt til uttalelse til Utviklings- og kompetanseetaten, Helseetaten, Bymiljøetaten, Barne- og familieetaten, Utdanningsetaten og Bydel Alna. I tillegg fikk ansvarlige byråder rapporten til uttalelse. Kommunerevisjonen har mottatt uttalelser fra alle reviderte virksomheter, samt respektive byråder eller byrådsavdelinger. Under oppsummerer og vurderer Kommunerevisjonen de viktigste punktene i de mottatte uttalelsene. Uttalelsene er som helhet lagt som vedlegg 4 i rapporten. Det fremgår ikke at uttalelsen fra Utviklings- og kompetanseetaten er elektronisk godkjent, men Kommunerevisjonen har fått dette dokumentert.

## 10.1 Byråden for finans

### 10.1.1 Uttalelsen fra byråden for finans

Byråden påpeker at finansbyråden både har ansvar for oppfølging av informasjonssikkerhet i virksomhetene under byrådsavdelingen, herunder Utviklings- og kompetanseetaten, og for den overordnede styringen av informasjonssikkerhet i kommunen. Byråden hadde ingen kommentarer til prosjektets revisjonskriterier, metode, kilder eller data. Byråden viser til at rapporten er nyttig og bekrefter hans inntrykk av behov for forbedringer på området. Han viser til at forbedringsbehovet også var bakgrunnen for forslaget i byrådets budsjett for 2017 om å etablere et informasjonssikkerhetsmiljø i Byrådsavdeling for finans. Det pekes videre på at byrådsavdelingen har iverksatt flere tiltak på området fra høsten 2017 og i 2018, blant annet er det utarbeidet en mal for databehandleravtale og kurs om informasjonssikkerhet i IKT-anskaffelser, samt kurs om risikovurderinger på informasjonssikkerhetsområdet.

Byråden viser til at byrådsavdelingen flere ganger underveis i utviklingen av HMSREG var blitt informert av Utviklings- og kompetanseetaten om at de i løpet av anskaffelsesprosessen hadde kontakt med Datatilsynet vedrørende informasjonssikkerhet.

Byråden skriver at han vil vurdere om kravene til informasjonssikkerhet er tilstrekkelige og godt nok forankret i virksomhetene, og påpeker at dette er spesielt viktig i lys av byrådets digitaliseringsambisjoner. Byråden oppgir at informasjonssikkerhet og personvern ved IKT-anskaffelser er et av satsningsområdene for 2019. Dette vil omfatte alle fasene i anskaffelsesprosessen. Revisjonsrapporten gir i denne forbindelse nyttig informasjon som vil bli benyttet i det videre arbeidet.

Byråden viser videre til at Utviklings- og kompetanseetaten gjennom tildelingsbrevet for 2019 skal lage og oppdatere maler for kontraktsstrategi, konseptutvalgsutredninger, behov- og kravspesifikasjon, avtaledokumenter og databehandleravtaler, slik at disse blant annet ivaretar hensynet til personvern og informasjonssikkerhet. Utviklings- og kompetanseetaten skal også utarbeide en veileder for å anskaffe skytjenester, slik at behov og krav til personvern og informasjonssikkerhet ivaretas. Etaten skal også utarbeide et sett av standardkrav til sikkerhetstester, samt maler og veiledere som skal sikre at krav til ROS-analyser og personvernkonsekvensanalyser ivaretas.

### 10.1.2 Kommunerevisjonens vurdering

Kommunerevisjonen merker seg at byråden peker på iverksatte og framtidige tiltak som framstår som relevante, og har ellers ingen kommentarer til byrådens uttalelse.

## 10.2 Byrådsavdeling for eldre, helse og arbeid

### 10.2.1 Uttalelsen fra Byrådsavdeling for eldre, helse og arbeid

Byrådsavdelingen angir at rapporten oppfattes som nyttig. Byrådsavdelingen har ingen innvendinger til undersøkelsens revisjonskriterier, metode, kilder eller data. Byrådsavdelingen viser til at rapportens anbefalinger vil bli lagt til grunn ved senere anskaffelser.

### 10.2.2 Kommunerevisjonens vurdering

Kommunerevisjonen merker seg at rapportens anbefalinger vil bli lagt til grunn ved senere anskaffelser, og har ellers ingen kommentarer til byrådsavdelingens uttalelse.

## 10.3 Byråden for miljø og samferdsel

### 10.3.1 Uttalelsen fra byråden for miljø og samferdsel

Byråden oppgir at hun oppfatter rapporten som nyttig og relevant. Hun påpeker at anbefalingene som gjelder samlet for de reviderte virksomhetene, er relevante også for Bymiljøetaten. Dette gjelder spesielt for anskaffelsen av *prosjekthotell*, men også sikkerhetssvakhetene som ble påvist i *saksbehandlingsverktøy beboerparkering*. Hun har ingen innvendinger til revisjonskriteriene, metode, kilder eller data, men viser til at sikkerhetsloven muligens kunne ha vært anvendt som kilde til revisjonskriterier i undersøkelsen. Byråden bemerker at det kanskje kunne vært tydeligere formulert i hovedproblemstillingen at undersøkelsen i hovedsak vurderte prosesskvalitet.

Byråden viser til at hun i 2019 vil følge opp undersøkelsens konklusjoner og anbefalinger med Bymiljøetaten, og viser til at dette spesielt gjelder anskaffelsene *prosjekthotell* og *saksbehandlingsverktøy beboerparkering.*

### 10.3.2 Kommunerevisjonens vurdering

Kommunerevisjonen merker seg byrådens kommentar til problemstillingen. Undersøkelsen har i hovedsak vært rettet mot prosesskvalitet. Kommunerevisjonen ønsket likevel å kunne vurdere vesentlige mangler ved kvaliteten på sikkerhetskrav, sikkerhetstesting mv. Dette er også gjort i noen tilfeller.

Kommunerevisjonen benyttet ikke sikkerhetsloven som kilde til kriterier da undersøkelsen ikke omfattet anskaffelser av systemer som var underlagt sikkerhetsloven.

Kommunerevisjonen merker seg at byråden i 2019 vil følge opp undersøkelsen i den formelle styringsdialogen med Bymiljøetaten.

## 10.4 Byråden for oppvekst og kunnskap

### 10.4.1 Uttalelsen fra byråden for oppvekst og kunnskap

Byråden oppga at rapporten med anbefalinger var nyttig i forbedringsarbeidet knyttet til informasjonssikkerhet. Byråden hadde ingen kommentarer til prosjektets metode, kilder eller data, og uttrykte at revisjonskriteriene framsto som relevante. Byråden påpeker at hovedproblemstillingen kunne vært tydeligere formulert ved oppstart, slik at det var klarere at undersøkelsen var rettet mot prosesskvaliteten, og ikke kvaliteten, ved sikkerhetskrav i IKT-anskaffelser. Byråden skriver samtidig at avgrensningen er godt begrunnet og undersøkelsen av prosesskvaliteten har stor verdi.

Byråden skriver at hun tar funnene i rapporten alvorlig, og at hun i 2019 vil følge opp undersøkelsen i den formelle styringsdialogen med Utdanningsetaten og Barne- og familieetaten. Dette for å sikre at anbefalingene vil bli lagt til grunn ved framtidige anskaffelser. Byråden viser til at hun vil be virksomhetene sikre at det finnes rutiner for å gjennomføre risikovurderinger i forkant av IKT-anskaffelser og at det gjennomføres tilstrekkelig testing og kontroll av at sikkerhetskravene er levert før nye løsninger settes i produksjon.

### 10.4.2 Kommunerevisjonens vurdering

Kommunerevisjonen merker seg at byråden i 2019 vil følge opp undersøkelsen i den formelle styringsdialogen med Utdanningsetaten og Barne- og familieetaten, og at byråden vil følge opp at det finnes rutiner for å gjennomføre risikovurderinger i forkant av IKT-anskaffelser og at det gjennomføres tilstrekkelig testing og kontroll av at sikkerhetskravene er levert før nye løsninger settes i produksjon. Vedrørende byrådens kommentar om undersøkelsens problemstilling, vises det til Kommunerevisjonens vurdering under 10.3.2.

## 10.5 Utviklings- og kompetanseetaten

### 10.5.1 Uttalelsen fra Utviklings- og kompetanseetaten

Utviklings- og kompetanseetaten har ingen innvendinger til informasjonen om prosjektets hensikt og revisjonskriteriene som er benyttet. Etaten kommenterer at det har vært uheldig for helhetsbildet at det ikke ble gjennomført intervjuer av deltagerne i de ulike anskaffelsene.

Utviklings- og kompetanseetaten skriver videre at den tar til etterretning at Kommunerevisjonen legger til grunn en større forventning til dokumentering av anskaffelsesprosessen, uavhengig av hvor avhengig virksomheten er av systemet (systemets kritikalitet), enn det etaten har lagt til grunn. Dette gjør at totalvurderingen fremstår som noe ubalansert.

Etaten mener at Kommunerevisjonens vurdering om at det varierte i hvilken grad det fremgikk vurderinger av beskyttelsesbehovet for dataene som systemene skulle behandle, var unyansert. Etaten viser til at det for anskaffelse av HMSREG og service management verktøy var gjennomført verdikartlegging hvor dataenes beskyttelsesbehov for konfidensialitet, integritet og tilgjengelighet var vurdert og dokumentert.

Etaten kommenterer at kontraktstrategiene for de tre anskaffelsene, som var blitt oversendt Kommunerevisjonen, inneholdt vurderinger av risiko. Etaten mener at dette ikke kommer frem i Kommunerevisjonens vurderinger. Etaten presiserer videre at det ved anskaffelsene av HMSREG og systemstøtte til innkjøpsanalyse var avsatt en egen informasjonssikkerhetsressurs.

Etaten presiserte at det ved anskaffelsene av Service Management verktøy og HMSREG var avgitt egen informasjonssikkerhetsresurs til anskaffelsesprosjektene.

Når det gjelder meldte tiltak etter rapporten, skriver Utviklings- og kompetanseetaten at det er blitt etablert en retningslinje i etatens styringssystem for å sikre at tilstrekkelige krav til sikkerhet i IKT-anskaffelser er satt. Retningslinjen skal ifølge etaten gjennom en godkjenningsprosess som skal sikre forankring i ledelsen og at retningslinjen blir kommunisert ut i organisasjonen. Etaten viser videre til at den planlegger å legge inn oppdatert veiledningstekst i mal for kontraktsstrategien i *Veileder for anskaffelser i Oslo*

*kommune*, hvor kravene til ivaretakelse og dokumentasjon av informasjonssikkerheten i IKT-anskaffelser kommer tydeligere frem. Etaten melder at begge tiltak skal gjennomføres i løpet av første kvartal 2019.

### 10.5.2 Kommunerevisjonens vurdering

Det er tydelige krav blant annet i lov og forskrift til dokumentasjon av anskaffelser og til risikovurderinger. Kommunerevisjonen valgte derfor å ta utgangspunkt i hva som forelå av slik dokumentasjon, og ba deretter om supplerende redegjørelser i form av skriftlige svar fra virksomhetene. Utviklings- og kompetanseetaten fikk anledning til å utdype ulike sider ved de undersøkte prosessene i to skriftlige spørrerunder, samt i tilknytning til at etaten fikk en samlet faktafremstilling til verifisering i oktober 2018. I en breddeundersøkelse som dette vil det være relativt ressurskrevende å gjennomføre egne intervjuer for hver anskaffelse. Kommunerevisjonen mener rapportens fakta-grunnlag er tilstrekkelig for å besvare undersøkelsens problemstilling, men merker seg at etaten mener det var uheldig at det ikke ble gjennomført intervjuer.

Utviklings- og kompetanseetaten har i uttalelsen en kommentar knyttet til Kommunerevisjonens forventninger til dokumentasjon av anskaffelsen. Kommunerevisjonen vil peke på at systemets beskyttelsesbehov påvirker behovet for risikovurderinger og dokumentasjon i den forbindelse. Særlig forventes omfanget av risikovurderinger å øke jo mer avhengig virksomheten er av systemet. Uavhengig av systemets beskyttelsesbehov forventes det likevel at risikovurderinger er gjennomført og dokumentert, i en systematisk prosess. Denne forståelsen ligger til grunn for Kommunerevisjonens vurderinger og konklusjoner.

Kommunerevisjonen merker seg at Utviklings- og kompetanseetaten mener Kommunerevisjonens vurdering om at det varierte i hvilken grad det fremgikk vurderinger av beskyttelsesbehovet for de ulike typene data, var unyansert. Kommunerevisjonen ser at det kunne vært tydeligere markert i vurderingen at svakhetene på dette området gjaldt én av de tre undersøkte anskaffelsene, og har justert teksten i vurderingen i kapittel 2 slik at dette er spesifisert.

For to av anskaffelsene dekker risikovurderingene i kontraktstrategien selve anskaffelsesprosessen, og ikke risikovurderinger av informasjonssikkerhet i systemet som skulle anskaffes. For det tredje systemet, HMSREG, inneholdt kontraktstrategien noen risikovurderinger knyttet til informasjonssikkerhet i systemet som skulle anskaffes. Det er på dette grunnlaget foretatt enkelte justeringer i faktafremstillingen og vurderingen for HMSREG.

Kommunerevisjonen har på bakgrunn av etatens opplysninger om avgitte informasjons-sikkerhetsressurser justert fremstillingen knyttet til Service Management verktøy i tabell 3 i kapittel 8. På samme grunnlag er det foretatt en mindre justering i kapittel 9.1.

Etter Kommunerevisjonens vurdering har Utviklings- og kompetanseetaten varslet tiltak som kan være relevante sett i lys av undersøkelsens anbefalinger og konklusjoner. I den sammenheng forstår Kommunerevisjonen etaten dithen at den nå har etablert retningslinjer for sikkerhetskrav i IKT-anskaffelser som omfatter hele anskaffelsesprosessen.

## 10.6 Helseetaten

### 10.6.1 Uttalelsen fra Helseetaten

Helseetaten har i tilbakemeldingen til Kommunerevisjonens rapport til uttalelse ingen innvendinger til Kommunerevisjonens undersøkelse.

Helseetaten melder som tiltak at den i større grad vil vektlegge risikovurderinger før utarbeidelse av krav til informasjonssikkerhet, og også i større grad vil dokumentere hvilke vurderinger som er gjort knyttet til sikkerhetstesting før nye systemer produksjonsettes. Etaten skriver at tiltakene skal iverksettes i tidligfase i pågående anskaffelser, og i kommende anskaffelser med tiltaksoppstart primo januar 2019.

### 10.6.2 Kommunerevisjonens vurdering

Etter Kommunerevisjonens vurdering har Helseetaten varslet relevante tiltak sett i lys av undersøkelsens anbefalinger og konklusjoner.

## 10.7 Bymiljøetaten

### 10.7.1 Uttalelsen fra Bymiljøetaten

Bymiljøetaten har i tilbakemeldingen til Kommunerevisjonens rapport til uttalelse ingen innvendinger til Kommunerevisjonens undersøkelse. Etaten peker på «at de sikkerhets-svakhetene som er omtalt på side 6 i rapporten [rapportens sammendrag] nå er utkvittert, noe som også fremgår i dokumentasjonen som er oversendt Kommunerevisjonen.»

Bymiljøetaten skriver at den i løpet av første halvår 2019 vil vurdere og eventuelt gjennomføre tiltak etter rapporten. Den viser videre til at tiltakene vil konkretiseres nærmere i en plan hvor etaten vil se hen til rapporten. Foreløpig vurderer Bymiljøetaten å foreta justeringer som ivaretar rapportens påpekninger når det gjelder rutiner for involvering og samarbeid på tvers av fagmiljøer, ved IKT-relaterte anskaffelser. Bymiljøetaten gir også tilbakemelding om at den har satt i gang et arbeid for å utvikle en ny anskaffelsesstrategi. Det vil også berøre forhold vedrørende kontraktsoppfølging og internkontroll. Rapportens funn vil bli vurdert også i denne prosessen.

### 10.7.2 Kommunerevisjonens vurdering

Kommunerevisjonen har mottatt dokumentasjon fra etaten som viser at det over tid var blitt arbeidet med å lukke sikkerhetsavvik også etter undersøkelsesperioden, og at det i mottatt dokumentasjon var utkvittert at avvik var blitt lukket. Kommunerevisjonen har imidlertid ikke tatt stilling til om alle avvik var lukket.

Etter Kommunerevisjonens vurdering har Bymiljøetaten varslet tiltak som synes relevante sett i lys av undersøkelsens anbefalinger og konklusjoner.

## 10.8 Barne- og familieetaten

### 10.8.1 Uttalelse fra Barne- og familieetaten

Barne- og familieetaten har ingen innvendinger til informasjonen om prosjektets hensikt og revisjonskriteriene som er benyttet.

Barne- og familieetaten kommenterer følgende når det gjelder etatens evaluering av leverandørs tilbud:

> Gjennomgang av Normen sjekkliste som inneholdt mer enn 200 punkter er gjennomført i flere møter høsten 2017 hvor leverandør Visma og intern driftsleverandør UKE i Oslo kommune har stilt med fagkompetanse med hensyn til å gi detaljert og helhetlig beskrivelse av sikkerhetsløsningene av systemet. Oppfyllelse av sikkerhetskrav er detaljert gjennomgått og evaluert i disse møtene, og hvert enkelt punkt er verifisert av personell med nødvendig fagkompetanse.
>
> I rapport til uttalelse kan det synes som om revisjonen har fått forståelse av at gjennomgang av Normen sjekklisten ble utført i ett møte 08.09.2017, noe som vil gi et noe feilaktig bilde av omfang og detaljnivå av evaluering av krav til informasjonssikkerhet i anskaffelsen. Dokumentasjon av de sikkerhetsmessige løsningene kunne dog vært bedre.

Vedrørende iverksatte tiltak etter rapporten skriver Barne- og familieetaten at den umiddelbart vil sikre at det gjennomføres ROS-analyser før gjennomføring av anskaffelser, samt forbedre evaluering og testing av sikkerhetskrav ved fremtidige IKT-anskaffelser. Etaten skriver videre at den i løpet av første halvår 2019 vil vurdere å gjennomføre ny sikkerhetstesting av den aktuelle anskaffelsen.

### 10.8.2 Kommunerevisjonens vurdering

Etaten kommenterer i sin uttalelse at gjennomgang av sjekkliste for Normen sammen med leverandør ble gjort i flere møter enn det ene der etaten har lagt frem referat. Kommunerevisjonen har føyd til en setning i faktabeskrivelsen om dette.

Når det gjelder etatens uttalelse om at oppfyllelse av sikkerhetskrav ble detaljert gjennomgått og evaluert i disse møtene, viser Kommunerevisjonen til vurderingen om at leverandørens løsningsspesifikasjon var så lite detaljert at den ikke var egnet som grunnlag for å evaluere de enkelte punktene i sjekklisten. Kommunerevisjonen mener at en tilstrekkelig detaljert skriftlig løsningsbeskrivelse er vesentlig for å kunne evaluere at sikkerhetskrav er hensyntatt.

Etter Kommunerevisjonens vurdering har Barne- og familieetaten varslet relevante tiltak sett i lys av undersøkelsens anbefalinger og konklusjoner.

## 10.9 Utdanningsetaten

### 10.9.1 Uttalelse fra Utdanningsetaten

Utdanningsetaten har i sin uttalelse ingen innvendinger til Kommunerevisjonens undersøkelse.

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

### 10.9.2 Kommunerevisjonens vurdering

Etter Kommunerevisjonens vurdering har Utdanningsetaten varslet tiltak som synes relevante sett i lys av undersøkelsens anbefalinger og konklusjoner.

## 10.10 Bydel Alna

### 10.10.1 Uttalelse fra Bydel Alna

Bydelen har i sin uttalelse ingen innvendinger til Kommunerevisjonens undersøkelse. Bydelen har i en e-post av 03.12.2018, som kom rett i etterkant av bydelens uttalelse, kommentert at innkjøpet av elektronisk låsesystem ved Furuset bibliotek og aktivitetshus ble foretatt sammen med Deichman bibliotek. Bydelen viser til at Furuset bibliotek og aktivitetshus er et samarbeidsprosjekt mellom bydel og Deichman, og at anskaffelsen ble foretatt via Deichman. Deretter inngikk andre tjenestesteder i bydelen avtale med samme leverandør uten å vurdere informasjonssikkerheten. Bydelen viser videre til at Furuset bibliotek og aktivitetshus aldri hadde planer om å ta i bruk bankkortmodulen siden utlån fra biblioteket er gratis.

Bydelen skriver i kommentarene til rapport til uttalelse at den tar Kommunerevisjonens anbefalinger til etterretning, og allerede har satt i gang tiltak i samsvar med disse. Bydelen viser blant annet til at den har opprettet informasjonssikkerhetskoordinatorer som skal arbeide med utforming av risikobaserte krav til informasjonssikkerhet ved anskaffelse av IKT-systemer og opprettet en stilling som rådgiver/controller på anskaffelsesområdet.

### 10.10.2 Kommunerevisjonens vurdering

Kommunerevisjonen merker seg bydelens tilbakemelding i e-post av 03.12.2018. Det er foretatt en justering i kapittel 7 for å tydeliggjøre at Deichman og bydelen sammen sto for innkjøpet av låsesystemet.

Etter Kommunerevisjonens vurdering har Bydel Alna varslet relevante tiltak sett i lys av undersøkelsens anbefalinger og konklusjoner.

# Referanser

### *a) Referanser fra Oslo kommune*

Byrådssak 1099.1/10: Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune

Byrådssak 1105/13: Instruks for informasjonssikkerhet

Byrådssak 1070/15: Instruks for virksomhetsstyring i Oslo kommune

Byrådssak 1057/17: Standard kontraktsvilkår for Oslo kommunes anskaffelser av varer, tjenester, bygg og anlegg

### *b) Eksterne referanser*

Lov av 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) (Opphevet)

Lov av 15.06.2018 nr. 38 om behandling av personopplysninger (personopplysningsloven)

Forskrift av 15.12.2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften)

Forskrift av 25.06.2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Forskrift av 12.08.2016 nr. 974 om offentlige anskaffelser (anskaffelsesforskriften)

Norm for informasjonssikkerhet – Helse- og omsorgstjenesten (Normen), 5. utgave, versjon 5.2, publisert juni 2016 og versjon 5.3, publisert juli 2018

Datatilsynets veileder om internkontroll og informasjonssikkerhet, publisert november 2009

Direktoratet for forvaltning og IKTs veileder om internkontroll i praksis – informasjonssikkerhet, publisert i februar 2016

ISO 27001, NS-EN ISO/IEC 27001:2017 Informasjonsteknologi – Sikringsteknikker – Ledelsessystemer for informasjonssikkerhet – Krav

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

# Tabelloversikt

# Vedlegg 1 Revisjonskriterier

I det følgende gjøres det nærmere rede revisjonskriterier og grunnlaget for disse. Revisjonskriterier er den målestokken som ligger til grunn for Kommunerevisjonens vurderinger.

Revisjonskriteriene er etablert for å kunne svare ut undersøkelsens vedtatte problemstillinger. Hovedproblemstillingen var som følger:

- Stiller kommunen gode og relevante sikkerhetskrav i anskaffelser på IKT-området?

Følgende var underproblemstillinger:

- Har de aktuelle virksomhetene vurdert behovet for sikkerhet i systemet som skal anskaffes?
- Har krav til sikkerhet blitt fulgt opp overfor leverandøren fram til systemet er implementert?

***Risikovurderinger og vurdering av sikkerhetsbehov***

***Revisjonskriterier:***

- Risikovurderinger av informasjonssikkerhet bør være gjennomført og dokumentert for alle IKT-anskaffelser.
  - Risikovurderingene bør bygge på vurderinger av kritikaliteten til systemet[3] og beskyttelsesbehovet til informasjonen i systemet. Risikovurderingene bør gi tilstrekkelig grunnlag for å etablere sikkerhetskrav i tråd med virksomhetens vurdering av eget behov og aktuelt regelverk. Vurdering av trusler og sårbarhet, samt anbefalte sikkerhetstiltak for systemet, bør også inngå i dette arbeidet.
- Krav til informasjonssikkerhet bør inngå i en eventuell kravspesifikasjon. Behovene for sikkerhet i systemet som virksomheten har identifisert bør være dekket av sikkerhetskravene.
- Statens standardavtale for aktuell type anskaffelser skal benyttes ved inngåelse av avtale for anskaffelser over kr 500 000 eks. mva.

Når det gjelder kriteriet om at risikovurderingene skal gi tilstrekkelig grunnlag for å etablere sikkerhetskrav, har Kommunerevisjonen i begrenset grad undersøkt kvaliteten på det substansielle innholdet i risikoanalysene som ligger til grunn for vurdering av sikkerhetsbehov. For å synliggjøre de dokumenterte og strukturerte vurderingene av risiko har vi benyttet betegnelsen *risikoanalyse*.

Kriteriene hadde følgende grunnlag:

I lov av 14.04.2000 nr. 31 om behandling av personopplysninger (personopplysningsloven) § 13 sies følgende:[4]

> Den behandlingsansvarlige og databehandleren skal gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.
>
> For å oppnå tilfredsstillende informasjonssikkerhet skal den behandlingsansvarlige og databehandleren dokumentere informasjonssystemet og sikkerhetstiltakene.

[3] Med *system* menes alle typer anskaffelser som omfatter en IKT-komponent der det kan være relevant å stille krav til informasjonssikkerhet.

[4] Loven er nå erstattet av en ny personopplysningslov. Den trådte i kraft 20.07.2018. Dette var etter Kommunerevisjonens undersøkelsesperiode.

I personopplysningsloven § 15 sies følgende:

> En databehandler kan ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse.
>
> I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.

Kommunerevisjonen la til grunn at de aller fleste anskaffelser av relevans for undersøkelsen ville være knyttet til systemer som behandlet personopplysninger, og at det i slike tilfeller burde utarbeides en databehandleravtale i forbindelse med anskaffelsen.

I Instruks for virksomhetsstyring i Oslo kommune sies følgende:

> Risikovurderinger skal utgjøre en sentral del av grunnlaget for å velge ut relevante sikkerhetstiltak. Vurdering av trusler og sårbarhet må inngå i dette arbeidet. Virksomhetens tiltak for å ivareta informasjonssikkerhet skal dokumenteres. [Pkt. 5.7.2]

I forskrift av 25.06.2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 sies følgende om forvaltningsorganer som benytter elektronisk kommunikasjon (andre og tredje avsnitt):

> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.
>
> Omfang og innretning på internkontrollen skal være tilpasset risiko.

I forskrift av 15.12.2000 nr. 1265 om behandling av personopplysninger (personopplysningsforskriften) § 2-4 sies følgende (første, andre og fjerde ledd):

> Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.
>
> Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.
>
> Resultatet av risikovurderingen skal dokumenteres.

I den grad det er strengere krav i annen særlovgivning til behandling av personopplysninger eller annen sensitiv informasjon, vil dette legges til grunn dersom dette er aktuelt.

*Norm for informasjonssikkerhet i Helse og omsorgssektoren* (Normen) er en bransjenorm som skal bidra til tilfredsstillende informasjonssikkerhet og personvern hos den enkelte virksomhet og i sektoren generelt, jf. Normen versjon 5.3 (20.07.2018), side 6 og versjon 5.2 (09.06.2016) side 1. Normen stiller krav som detaljerer og supplerer gjeldende regelverk på området. Blant annet omfatter normen krav til innhold i avtale med databehandlere og leverandører, jf. versjon 5.4 kapittel *5.7 leverandørforhold og avtaler* og versjon 5.2 kapittel *5.8 Avtaler*.

I Instruks for informasjonssikkerhet i Oslo kommune sies følgende:

> Risikovurdering skal være en sentral del av arbeidet med sikkerhetstiltak. Konkrete sikkerhetstiltak skal bygge på anbefalte sikkerhetskrav i mal for egenerklæring og dokumenterte risikovurderinger. [Pkt. 3.3]
>
> Alle virksomheter må kartlegge og verdivurdere informasjon som må beskyttes i henhold til integritet, konfidensialitet eller tilgjengelighet. [Pkt. 4.2]
>
> Oversiktene over rettslige krav og verdivurdert informasjon må brukes som grunnlag for vurdering og prioritering av sikkerhetstiltak i den enkelte virksomhet og for fellesystemer, sektorsystemer og andre ikke-virksomhetsspesifikke systemer. [Pkt. 4.3]
>
> Krav knyttet til informasjonssikkerhet må ivaretas allerede ved planlegging av anskaffelser av systemer. [Pkt. 5.4 a)]
>
> Krav til sikkerhet må inngå i kravspesifikasjon og andre avtaledokumenter, herunder databehandleravtale etter personopplysningsloven § 13. [Pkt 5.4 b)]

I Reglement for informasjons- og kommunikasjonsteknologi og informasjonssikkerhet i Oslo kommune sies følgende:

> Virksomhetsleder må sørge for at leverandører det inngås avtale med om behandling av personopplysninger oppfyller kravene til informasjonssikkerhet i henhold til lov og regelverk på informasjonssikkerhetsområdet. [§8, pkt. 2b)]

I byrådssak 1057/17, Standard kontraktsvilkår for Oslo kommunes anskaffelser av varer, tjenester, bygg og anlegg, av 23.05.2017, sies følgende:

> Følgende standardkontrakter vedtas for Oslo kommune: […] Statens standardkontrakter for IT-anskaffelser. (Den av Statens standardavtaler for IT-anskaffelser som er mest anvendelig skal benyttes.) og tilhørende bilagsformular […] [Pkt. 1]
>
> […]
>
> Alle virksomheter som er en del av rettssubjektet Oslo kommune pålegges å bruke vedtatte standardkontrakter, med tilhørende kontraktsformularer/bilagsformular der slike er utarbeidet, når de foretar anskaffelser av varer, tjenester eller bygg og anlegg til en verdi over kr 500 000 på områder som omfattes av standardkontraktene. [Pkt. 10]

***Evaluering og kontroll av stilte sikkerhetskrav***

Revisjonskriterier:

- Tilbyders tilbakemelding på eventuelle krav til informasjonssikkerhet som stilles i tildelingskriterier skal evalueres av oppdragsgiver.
- Før produksjonssetting skal det sørges for kontroll av at systemet overholder stilte informasjonssikkerhetskrav, herunder gjennomføring av relevante sikkerhetstester. Kontrollen av sikkerhetskrav bør dokumenteres.

Kriteriene har følgende grunnlag:

Krav til tildelingskriterier omtales blant annet i anskaffelsesforskriften § 8-11 (anskaffelser under EØS-terskelverdi) og § 18-1 (anskaffelser over EØS-terskelverdi). Etter disse bestemmelsene skal oppdragsgiver velge tilbud på grunnlag av kriteriene.

Som beskrevet over, stiller eForvaltningsforskriften § 15 krav til internkontroll (styring og kontroll) på informasjonssikkerhetsområdet.

Videre sies det i *Instruks for informasjonssikkerhet i Oslo kommune*, byrådssak 1105/13 av 17.10.2013 følgende:

> Systemers sikkerhetsfunksjonalitet må testes før produksjonssetting og versjons-oppgradering… [Pkt. 5.4 c)]
>
> Systemeier må sørge for nødvendig kontroll av at avtalte sikkerhetskrav overholdes. [Pkt 5.4 e)]

I pkt. 5.7.2 i *Instruks for virksomhetsstyring i Oslo kommune* stilles det krav om at virksomheten dokumenterer tiltak for å ivareta informasjonssikkerhet. Dette innebærer at dokumentasjon av sikkerhetstiltak i anskaffelsesfasen bør ivaretas ved at man dokumenterer sikkerhetskravene og kontrollen av at disse er etterlevd.

***Deskriptiv analyse***
Følgende problemstillinger er belyst deskriptivt i undersøkelsen:

- Gjøres det vurderinger av leverandørenes modenhet og evne til å levere i henhold til krav på informasjonssikkerhetsområdet?
- Er det benyttet særskilt informasjonssikkerhetskompetanse i anskaffelser på IKT-området?

I undersøkelsen ble det også redegjort for om eiendomsrett til data og systemer er regulert i avtalen.

# Vedlegg 2 Metode

***Generelt om forvaltningsrevisjon***
De sentrale elementene i undersøkelsesmetoden er like i alle forvaltningsrevisjoner. Vi følger den gjeldende standarden for forvaltningsrevisjon i kommuner og fylkeskommuner i Norge (RSK 001). Med utgangspunkt i problemstillingen som ligger i oppdraget fra kontrollutvalget, har vi utledet relevante revisjonskriterier. Deretter har vi gjennomført den nødvendige innsamling, bearbeiding og analyse av data. Vi har så vurdert fakta opp mot revisjonskriteriene. Disse vurderingene har ledet fram til Kommunerevisjonens konklusjoner og anbefalinger.

***Beskrivelse av prosjektgjennomføringen***
Kommunerevisjonen har rettet undersøkelsen mot Barne- og familieetaten, Bydel Alna, Bymiljøetaten, Helseetaten, Utdanningsetaten og Utviklings- og kompetanseetaten, samt respektive byrådsavdelinger.

Det ble sendt ut oppstartsbrev til virksomheter og byrådsavdelinger i april/mai 2018. Oppstartsmøter ble avholdt i mai/juni 2018. I den forbindelse ble det i oppstartsmøte med Byrådsavdeling for finans og Utviklings- og kompetanseetaten særlig viet tid til avklaringer av enkelte ansvarsforhold på feltet. I tillegg ble det i oppstartsmøter og korrespondanse i den forbindelse gjort avklaringer om valg av anskaffelser, i tillegg til at det ble informert om undersøkelsens metode og fremdrift.

I juli 2018 ble et utkast til revisjonskriterier sendt virksomhetene for tilbakemelding. Det ble også sendt ut en forespørsel om diverse dokumenter og redegjørelser i tilknytning til de valgte anskaffelsene. Datainnsamlingsperioden var i hovedsak fra juni 2018 til oktober 2018.

Utkast til faktafremstilling ble sendt 18.10.2018 til de reviderte virksomhetene. Vi mottok i hovedsak tilbakemelding fra virksomhetene uken etter.

Kommunerevisjonen ga en muntlig presentasjon av rapportens vurderinger og konklusjoner til reviderte virksomheter og byrådsavdelinger i møte 08.11.2018.

Rapporten ble sendt til uttalelse 20.11.2018 til reviderte virksomheter og respektive ansvarlige byråder. Kommunerevisjonen mottok medio desember 2018 tilbakemeldingene fra virksomhetene og byrådene. Tilbakemeldingene medførte enkelte mindre endringer i rapporten. Ved korrekturlesing av rapporten ble det også avdekket en unøyaktighet i sammendraget som ble rettet.

***Valg av reviderte virksomheter og anskaffelser***
Undersøkelsen har vært rettet mot seks virksomheter og respektive byrådsavdelinger. Tabell 4 gir en oversikt over anskaffelsene som inngår i revisjonen og hvilken virksomhet som har foretatt anskaffelsene. Enkelte anskaffelser har hatt en annen prosjekteier enn anskaffende virksomhet, dette har gjerne vært en byrådsavdeling. I tillegg har Utviklings- og kompetanseetaten hatt en støtterolle i enkelte anskaffelser. Informasjon om disse forholdene fremkommer i det enkelte kapittel.

***Tabell 4 Oversikt over virksomheter og systemer som inngår i revisjonen***

| Virksomhet | System |
|---|---|
| Utviklings- og kompetanseetaten | HMSREG – Kjernesystem for leverandøroppfølging |
| | Systemstøtte til innkjøpsanalyse |
| | Service Management verktøy |
| Helseetaten | GPS lokaliseringsteknologi |
| | Ledelsesinformasjonsverktøy (LIV) |
| | Kvalitetsstyrings- og internkontrollsystem |
| Bymiljøetaten | Rammeavtale prosjekthotell |
| | Kontrollverktøy parkering |
| | Saksbehandlingsverktøy beboerparkering |
| Barne- og familieetaten | Visma flyt barnevernvakt |
| Utdanningsetaten | Tjeneste for vurdering og kartlegging av læring |
| | Toveis meldingstjeneste for Osloskolen |
| | Fagsystem for Pedagogisk-psykologisk tjeneste (PPT) |
| Bydel Alna | JodaCare |
| | Elektronisk låsesystem og bookingavtale |

For å sikre undersøkelsens relevans ble nyere anskaffelser valgt ut. Anskaffelsene ble videre valgt ut for å sikre en bredde av typer systemer, det være seg skytjenester, større fagsystemer og mer begrensede applikasjoner. Aktuelle anskaffelser ble i hovedsak identifisert gjennom søk i Doffin. Søkene ble avgrenset til å gjelde anskaffelser i IKT-relaterte kategorier med tilbudsfrist i 2016 eller senere. Totalt ble det identifisert ca. 70 aktuelle anskaffelser. Svært få anskaffelser på Doffin var publisert av bydeler. Grunnen til dette kunne være at bydelene gjorde avrop på inngåtte rammeavtaler og foretok anskaffelser under terskelverdi for kunngjøring. For å identifisere aktuelle anskaffelser foretatt fra bydeler benyttet vi KMD innkjøpsanalyse, som er et analyseverktøy for kommunens innkjøp, og Utviklings- og kompetanseetatens oversikt over IKT-systemer for å identifisere aktuelle anskaffelser.

Virksomhetene ble valgt ut for å dekke variasjon i erfaring med IKT-anskaffelser. Utviklings- og kompetanseetaten, Helseetaten og Utdanningsetaten ble ansett for å være store IKT-anskaffere med betydelige informasjonssikkerhetsmiljøer. Barne- og familieetaten og Bydel Alna ble regnet for å være virksomheter med relativt lite erfaring på IKT-anskaffelser. Bymiljøetaten er en virksomhet med forholdsvis mange IKT-anskaffelser, men med et lavere omfang enn de tre store IKT-anskafferne.

Før anskaffelsene ble valgt ut oversendte vi oversikter over aktuelle anskaffelser til virksomhetene, og ba om tilbakemelding på om det var grunner til ikke å velge anskaffelsene. Vi ønsket først og fremst informasjon om noen av anskaffelsene var kommet så kort at sikkerhetskrav ikke var utarbeidet, eller om anskaffelsene var avbrutt. Kommunerevisjonen foretok deretter en endelig vurdering av hvilke anskaffelser som skulle inngå i undersøkelsen.

### *Undersøkelsesperiode*

Undersøkelsesperioden har vært styrt av tidslinjen i de valgte anskaffelsene. Vi har som hovedregel valgt anskaffelser som startet opp etter 2015. Imidlertid har mange anskaffelser hatt en lengre historikk, slik at hendelser før 2015 i noen tilfeller er beskrevet. Kommunerevisjonen har valgt å ha undersøkelsesperioden frem til medio mai 2018, det vil si at forhold etter den tid ikke har blitt revidert. På dette tidspunktet fikk de reviderte virksomhetene informasjon om hvilke anskaffelser som kunne inngå i undersøkelsen. Vi har likevel valgt å beskrive enkelte hendelser etter mai 2018, dels for

å sikre en mer komplett fremstilling av anskaffelsesforløpet, og dels for å tydeliggjøre revisjonsbevis i de tilfellene det var relevant.

***Undersøkelsens datagrunnlag og metode for dataanalyse***
Datagrunnlaget i undersøkelsen har i hovedsak bestått av anskaffelsesrelatert dokumentasjon for de valgte IKT-anskaffelsene. Dette dreide seg blant annet om

- dokumenter som belyste arbeidet med planleggingen av anskaffelsen slik, som kontraktstrategi, risikovurderinger, styringsdokumenter o.l.
- kvalifikasjonsgrunnlag, konkurransegrunnlag og kontrakter med bilag
- leverandørenes tilbud og evaluering av tilbudene
- kontroll- og testdokumentasjon
- redegjørelser fra virksomhetene knyttet til arbeidet med anskaffelsene

Analyseverktøyet Nvivo ble benyttet for å gjennomføre spørringer på data og til en viss grad benyttet til koding av data.

***Gyldighet og pålitelighet***
Gyldighet brukes gjerne som et uttrykk for om vi har målt det vi ønsker å måle, det vil si om de innsamlede data er tilstrekkelig relevante og dekkende for problemstillinger og konklusjoner. Pålitelighet er et uttrykk for hvor nøyaktig innsamlingen av data har vært, og for at det ikke er skjedd systematiske feil underveis i innsamlingen.

I denne undersøkelsen er faktagrunnlaget i hovedsak hentet fra dokumenter fra utvalgte anskaffelser og fra redegjørelser fra de reviderte virksomhetene om disse anskaffelsene. Datagrunnlaget er ment å gi gyldig informasjon om disse anskaffelsene, og er ikke ment å være tilstrekkelig til å gi en fullstendig fremstilling av de utvalgte virksomhetenes praksis på området. Kommunerevisjonens vurderinger og konklusjoner er tilpasset dette, i tråd med problemstillingene i undersøkelsen.

Det ligger videre en begrensning i at dette er en breddeundersøkelse av flere anskaffelser, og ikke en dybdeundersøkelse av noen få. En konsekvens av dette er at vi ikke har undersøkt alle aspekter ved anskaffelsene som kan ha betydning for informasjons-sikkerheten i systemene som er anskaffet, men har konsentrert oss om det vi har vurdert som de viktigste prosessene. Dette er hensyntatt i valg av revisjonskriterier og i våre vurderinger og konklusjoner.

Vi har søkt å avklare status på de ulike skriftlige kildene som er benyttet, og å kontrollere ulike kilder opp mot hverandre. Videre er Kommunerevisjonens fakta-beskrivelse verifisert av virksomhetene. Dette bidrar til å redusere risikoen for at vi har gjengitt informasjon som ikke er korrekt, eller har misforstått de skriftlige kildene. Informasjon som stammer fra redegjørelser fra virksomhetene er i tillegg i hovedsak kontrollert opp mot andre skriftlige kilder. I tilfeller der dette ikke har vært mulig innenfor rammene av undersøkelsen, går dette frem av faktafremstillingen.

Rapporten har vært underlagt intern kvalitetssikring i Kommunerevisjonen. Samlet sett mener vi at datagrunnlaget i undersøkelsen gir et tilfredsstillende pålitelig og gyldig grunnlag for våre vurderinger og konklusjoner.

# Vedlegg 3 Begrepsforklaring

| Begrep | Forklaring |
|---|---|
| Akseptansetest | Formalisert test av programmer/applikasjoner for å undersøke om brukerbehov og funksjonelle krav er tilfredsstilt. |
| Applikasjon | Et dataprogram utviklet for å la brukeren gjennomføre bestemte aktiviteter, for eksempel tekstbehandling, saksbehandling eller nettlesing. |
| ISAE 3000 (type 2) | Internasjonal standard for attestasjonsoppdrag som ikke er revisjon eller forenklet revisorkontroll av historisk finansiell informasjon. Rapporter av type 2 beskriver operasjonell effekt av kontrollrammeverk over en periode på seks måneder. I tilfellet det vises til i rapporten (jf. kapittel 6.2.3) gjaldt det generelle IT-kontroller i leverandørens IT-miljø. |
| ISO 27000-serien | En serie internasjonale standarder som omhandler ulike aspekter av informasjonssikkerhet. |
| ISO 27001 | En internasjonal standard som spesifiserer krav til styringssystemer for informasjonssikkerhet. |
| ISO 27002 | En internasjonal standard som gir anbefalinger basert på beste praksis for tiltak for informasjonssikkerhet. |
| Konkurranse med forhandling | En prosedyre for anskaffelser som tillater oppdragsgiveren å forhandle om tilbudene. |
| Kritikalitet | Kritikaliteten til et system (evt. data eller tjeneste) angir i hvilken grad man er avhengig av systemet. Dersom et system har høy kritikalitet for en virksomhet, betyr dette at virksomhetens evne til å gjennomføre sine sentrale oppgaver blir vesentlig redusert ved bortfall av systemet. |
| Redundans | Duplisering av kritiske komponenter og funksjoner. |
| Risikoanalyse | En strukturert og dokumentert prosess for å identifisere og forstå risiko og risikonivå. |
| Risikoakseptanse-kriterier | Kriterier som forteller hvor høyt risikonivå som kan aksepteres. |
| Risikomatrise | Tabell som definerer risikonivå som funksjon av en sannsynlighet/hyppighet og en konsekvensverdi. |
| Risikonivå | Risikonivået angir hvor stor en risiko er. For en hendelse (risikoscenario) defineres risikonivået gjerne basert på sannsynligheten til hendelsen (eller forventet hyppighet) og konsekvensen av hendelsen. |
| SSA | Statens Standardavtaler: kontraktsmaler for kjøp av IT og konsulenttjenester utarbeidet av Difi. |
| SSA-B | Bistandsavtalen. Egnet for konsulentkjøp når man har behov for kompetanse, men ikke har utarbeidet kravspesifikasjon som definerer et sluttresultat/behov. |
| SSA-D | Driftsavtalen. Egnet for kjøp av driftstjenester for IT-systemer, regulerer et vidt spekter av driftssituasjoner med fokus på standardiserte driftstjenester. |
| SSA-K | Kjøpsavtalen. Egnet for kjøp av standard IT-utstyr eller standard programvare som ikke skal tilpasses virksomheten, evt. med mindre kundetilpasninger. |
| SSA-L | Avtale om løpende tjenestekjøp. Egnet for kjøp av løpende tjenester over internett, inkludert standardiserte skytjenester. |
| SSA-O | Oppdragsavtalen. Egnet for utrednings- og utviklingsoppgaver. |

| | |
|---|---|
| SSA-T | Utviklings- og tilpasningsavtalen. Egnet for kjøp av programvare som skal utvikles eller tilpasses dersom kunden ikke på forhånd kan spesifisere nøyaktig hvordan programvaren skal utvikles/tilpasses. |
| SSA-V | Vedlikeholdsavtalen. Egnet for levering av vedlikehold og service for programvare og/eller utstyr, samt lisensutvidelser, kompletteringskjøp etc. |
| Skytjeneste | Databasert tjeneste som er tilgjengelig fra eksterne servere tilknyttet internett, gjerne utenfor brukerens egen virksomhet. |
| Tilgangsstyring | Styring av tilgang til data og informasjon, gjerne basert på roller og tjenstlig behov. Inkluderer vanligvis logging av tilganger. |
| Tjenestenektangrep | Et angrep som søker å gjøre en internett-basert tjeneste utilgjengelig ved å oversvømme den med falske forespørsler. Også kjent som DoS- (Denial of Service) og DDoS- (Distributed Denial of Service) angrep. |

# Vedlegg 4 Uttalelser til rapporten

Oslo kommune
**Byrådsavdeling for finans**

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

**Unntatt offentlighet**
Offl § 5 andre ledd

Dato: 19.12.20189

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| 18/00378-78 | 201802613-24 | Atle H. Hjelkerud, 412 90 275 | 126 |

**RAPPORT TIL UTTALELSE - FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Jeg viser til Kommunerevisjonens brev av 20.11.2018 med rapport til uttalelse etter forvaltningsrevisjonen av sikkerhetskrav i et utvalg IKT-anskaffelser. Gjennom undersøkelsen har kontrollutvalget satt fokus på et svært viktig område for kommunen. Rapporten bekrefter inntrykket av at det er behov for forbedringer på området og gir støtte for vår prioritering av sikkerhetskrav i anskaffelsesprosesser som et satsingsområde for fagmiljøet for informasjonssikkerhet i Byrådsavdeling for finans i 2019.

I det følgende besvares Kommunerevisjonens spørsmål.

**1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?**

Informasjonen om prosjektets hensikt anses tilstrekkelig klar.

**2. Har byråden kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?**

Jeg har ingen kommentar til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner, utover at de fremstår relevante for undersøkelsen.

**3. Har byråden kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?**

Jeg har ingen kommentarer til revisjonskriteriene som ligger til grunn for konklusjonene.

**Byrådsavdeling for finans**
Postadresse:
Rådhuset, 0037 Oslo

E-post: postmottak@byr.oslo.kommune.no
Org.nr.:

**4. Hva er byrådens samlede vurdering av rapportens konklusjoner og anbefalinger?**

Rapporten er nyttig og bekrefter mitt inntrykk av behovet for forbedringer på området, noe som også var bakgrunnen for byrådets budsjett for 2017 hvor vi foreslo å etablere informasjonssikkerhetsmiljøet i Byrådsavdeling for finans.

Anskaffelsene som er revidert ble i all hovedsak gjennomført i perioden 2015-2017. Informasjonssikkerhetsmiljøet i Byrådsavdeling for finans ble etablert og startet sitt arbeid i 2017. Det har vært stort fokus på å heve kompetansen blant ledere og ansatte, og forbedre kommunens styringsevne på informasjonssikkerhetsområdet. For 2019 er et av satsningsområdene informasjonssikkerhet og personvern ved IKT-anskaffelser, det vil si alle fasene i anskaffelsesprosessen, fra kontraktsstrategi, anskaffelse, produksjonssetting, forvaltning og utfasing. Revisjonsrapporten gir i denne forbindelse nyttig informasjon som vil bli benyttet i det videre arbeidet.

**5. Vil byråden vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?**

Som finansbyråd har jeg ansvar både for oppfølging av informasjonssikkerhet i FINs sektor, og for den overordnede styringen av informasjonssikkerhet i kommunen.

Byrådsavdeling for finans har allerede iverksatt en rekke tiltak på området, og vil iverksette flere tiltak framover. Tiltakene retter seg mot kommunens virksomheter generelt. Enkelte tiltak retter seg mot FINs egen sektor. Samtidig understrekes det at UKE er i en særstilling blant kommunens virksomheter, ved at de anskaffer IKT-systemer som ofte skal benyttes av flere virksomheter på tvers av sektorene. Dermed vil tiltakene som iverksettes overfor UKE også ha betydning utover FINs egen sektor.

Tiltakene ble hovedsakelig iverksatt fra høsten 2017 og videre i 2018, og kan derfor ikke ha hatt effekt for anskaffelsene som er revidert i rapporten, som i all hovedsak ble gjennomført i perioden 2016-2017.

Blant hovedtiltak som vi allerede har iverksatt på kommunebasis kan følgende nevnes:

Byrådsavdeling for finans har utarbeidet mal for databehandleravtaler. Malen sørger for at det blir stilt like krav til informasjonssikkerhet til kommunens databehandlere. Det er imidlertid en utfordring at ikke alle virksomheter benytter malen i sine anskaffelser. Jeg vil vurdere behovet for tiltak som kan sørge for en bedre forankring av malen i virksomhetene, slik at den i større grad blir tatt i bruk. Det vil også bli utarbeidet en forenklet versjon av malen for databehandleravtale, til bruk i de tilfeller dette er hensiktsmessig.

Byrådsavdeling for finans tilbyr kostnadsfritt opplæringsaktiviteter, maler og veiledninger for kommunens virksomheter. Egne kurs om informasjonssikkerhet i forbindelse med IKT-anskaffelser har vært avholdt flere ganger. I tillegg ble det i sikkerhetsmånedene både i 2017 og i 2018 tilbudt foredrag for ledergrupper om informasjonssikkerhet og sikkerhetskrav ved IKT-

anskaffelser. Vi har også utviklet metodikk og tilbyr kurs i gjennomføring av risikovurderinger på informasjonssikkerhetsområdet mer generelt.

Jeg vil vurdere om kravene til sikkerhet er tilstrekkelige og godt nok forankret i virksomhetene. Dette er spesielt viktig i lys av byrådets digitaliseringsambisjoner.

Gjennom tildelingsbrevet til UKE for 2019, er det stilt krav om at UKE, i samarbeid med FIN, skal lage og oppdatere maler for kontraktsstrategi, konseptutvalgsutredninger, behov- og kravspesifikasjon, avtaledokumenter og databehandleravtaler, slik at disse blant annet ivaretar hensynet til personvern og informasjonssikkerhet, samt krav i ny sikkerhetslov. UKE skal også utarbeide en veileder for å anskaffe skytjenester, slik at behov og krav til personvern og informasjonssikkerhet ivaretas. Det skal utarbeides et sett av standardkrav til sikkerhetstester, samt maler og veiledere som skal sikre at krav til ROS-analyser og personvernkonsekvensanalyser (DPIA) ivaretas, både i virksomheten og i prosjekter, samt hos leverandører og deres underleverandører. Målet er at maler og veiledere skal benyttes i alle anskaffelser.

Jeg vil også vise til Oslo kommunes anskaffelsesstrategi, som ble vedtatt høsten 2017. Anskaffelsesstrategien skal bidra til felles overordnet tenkning og atferd i kommunens virksomheter, slik at anskaffelser blir et effektivt virkemiddel i arbeidet med å gi innbyggere og næringsliv gode løsninger og tjenester i tråd med dagens og fremtidens behov. Anskaffelsesstrategien inneholder felles overordnede mål og føringer som virksomhetene må følge i sine anskaffelser. Det er for eksempel et krav at kontraktsstrategi skal utarbeides tidlig i en anskaffelsesprosess. Kontraktsstrategien skal synliggjøre risikovurderinger og kritiske suksessfaktorer for den aktuelle anskaffelsen, og hensynet til informasjonssikkerhet tillegges tilstrekkelig vekt i de vurderingene som foretas.

I tiden framover vil det bli viktig å jobbe for at sikkerhet blir et fokusområde i alle faser av IKT-anskaffelser, fra planlegging til produksjonssetting, i løpende forvaltning og avslutning.

*HMSREG*

HMSREG er et elektronisk system for leverandøroppfølging. Systemet ble anskaffet på bakgrunn av en anskaffelsesprosess som startet med en leverandørkonferanse og en-til-en-møter med de leverandører som meldte sin interesse. Deretter ble det gjennomført en prekvalifisering, etterfulgt av en konkurranse med forhandling. Det fantes ingen løsninger som var ferdigutviklet, og Oslo kommune v/ Utviklings- og kompetanseetaten måtte selv være med på å utvikle løsningen (HMSREG) sammen med valgte leverandør. Denne anskaffelsen skiller seg fra kjøp av hyllevare eller en allerede eksisterende løsning, der sikkerhetskravene kan konkretiseres mye tidligere i anskaffelsesprosessen.

Byrådsavdeling for finans har flere ganger underveis i utviklingen av HMSREG blitt informert av UKE om at de i løpet av anskaffelsesprosessen har hatt kontakt med Datatilsynet, for å sikre ivaretakelse av informasjonssikkerhetshensyn.

**6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?**

Tiltakene er dels iverksatt allerede, resten iverksettes fortløpende gjennom 2019 og 2020.

**7. Oppfattes rapporten som nyttig for kommunen? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.**

Ja, se ovenfor.

**8. Hvordan vurderes rapportens oppbygning og språkbruk?**

Rapporten er ryddig og oversiktlig bygd opp. Språkbruken er klar og lett forståelig.

Med hilsen

Robert Steen
byråd for finans

*Godkjent elektronisk*

Oslo kommune
**Byrådsavdeling for eldre, helse og arbeid**

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Dato: 18.12.2018

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| 18/00378-78 | 201802613-27 | Stein Schatvet, 48 12 81 12 | 126 |

**RAPPORT TIL UTTALELSE - FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Vi viser til deres brev av 20.11.2018 der dere ber om byrådens vurdering av deres rapport fra forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser.

Forvaltningsrevisjonen omfatter i alt 15 IKT-anskaffelser hvorav tre der Byrådsavdeling for eldre, helse og arbeid er systemeier. Disse tre er GPS lokaliseringsteknologi, Ledelsesinformasjonsverktøyet LIV og Kvalitets- og internkontrollsystemet EQS.

Undersøkelsen viste at det ble gjennomført risikovurdering i forkant av anskaffelsen av Kvalitets- og internkontrollsystemet, mens dette ble gjennomført først senere i de to andre anskaffelsene. Det var stilt sikkerhetskrav i alle de tre anskaffelsene. I GPS anskaffelsen ble det benyttet en avtalemal som ikke var tilpasset det faktum at deler av løsningen skulle leveres som en skytjeneste.

På undersøkelsestidspunktet var det bare anskaffelsen av Ledelsesinformasjonssystem som var ferdigstilt, og i denne anskaffelsen var leverandørens tilbakemelding på sikkerhetskravene evaluert. Det ble imidlertid ikke gjennomført egne sikkerhetstester av Ledelsesinformasjonssystemet etter at det var levert.

Her er svar på de spørsmålene dere stilte i dere brev:

1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?

   Svar: Ja

2. Har byråden kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?

   Svar: Nei

**Byrådsavdeling for eldre, helse og arbeid**
Postadresse:
Rådhuset, 0037 Oslo
E-post: postmottak@byr.oslo.kommune.no
Org.nr.: 876819872

3. Har byråden kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?

   Svar: Nei

4. Hva er byrådens samlede vurdering av rapportens konklusjoner og anbefalinger?

   Svar: Rapporten gir et riktig bilde av den faktiske situasjon og anbefalingene syntes å være i samsvar med beste praksis på området.

5. Vil byråden vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?

   Svar: Rapportens anbefalinger vil bli lagt til grunn ved senere anskaffelser.

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?

   Svar: Se svar på foregående spørsmål

7. Oppfattes rapporten som nyttig for kommunen? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.

   Svar: Ja. Rapporten bidrar bl.a. til økt bevissthet om viktigheten av grundige risikovurderinger i forhold til informasjonssikkerhet og personvern allerede før kravspesifikasjonen utarbeides og konkurransedokumentene lages.

8. Hvordan vurderes rapportens oppbygning og språkbruk?

   Svar: Som god og lett forståelig.

Med hilsen

Svein Lyngroth
konst. kommunaldirektør

Kari Elisabeth Sletnes
konst. seksjonssjef

***Godkjent elektronisk***

Oslo kommune
**Byrådsavdeling for miljø og samferdsel**

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

**Unntatt offentlighet**
Offl § 14 første ledd

Dato: 17.12.2018

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| 18/00378-78 | 201802613-26 | Ingun Elde Spjelkavik, | 126 |

**RAPPORT TIL UTTALELSE - FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Jeg viser til Kommunerevisjonens brev av 20. november 2018 hvor det bes om tilbakemelding på forvaltningsrevisjonen *Sikkerhetskrav i IKT-anskaffelser* i Bymiljøetaten. I brevet stilles det flere spørsmål som ønskes besvart. Nedenfor følger mine kommentarer til rapporten.

**Byrådens vurdering av rapporten, dens konklusjoner og anbefalinger**

1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?

Svar: Jeg oppfatter at prosjektets hensikt har vært klar. Jeg vil også føye til at det er positivt at Kommunerevisjonen har gjennomført en forvaltningsrevisjon som «speiler» tiden så godt. Undersøkelsen er aktuell og viktig. Følgende hovedproblemstilling har blitt belyst: *Stiller kommunen gode og relevante sikkerhetskrav i anskaffelser på IKT-området*? Det kunne kanskje vært tydeligere i hovedproblemstillingen at Kommunerevisjonens undersøkelse i hovedsak har vurdert prosesskvalitet i denne undersøkelsen.

2. Har byråden kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?

Svar: Jeg merker meg de avgrensningene som har blitt gjort, og har ingen øvrige kommentarer.

3. Har byråden kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?

Svar: Revisjonskriteriene fremstår relevante og riktige. Det er mulig Sikkerhetsloven kunne vært anvendt som revisjonskriterium i denne revisjonen. Loven gjelder for statlige, fylkeskommunale og kommunale organer, og regulerer blant annet informasjonssikkerhet.

**Byrådsavdeling for miljø og samferdsel**

Postadresse:

Rådhuset, 0037 Oslo

E-post: postmottak@byr.oslo.kommune.no
Org.nr.:

Jeg merker meg for øvrig at den nye personopplysningsloven fra juli ikke ble brukt som revisjonskriterium, noe som fremstår fornuftig da denne ble vedtatt etter Kommunerevisjonens undersøkelsesperiode.

4. Hva er byrådens samlede vurdering av rapportens konklusjoner og anbefalinger?

Svar: Rapportens konklusjoner / vurderinger er klare ut fra funnene. Anbefalingene som gjelder samlet for de reviderte virksomhetene, er relevante også for Bymiljøetaten. Dette gjelder spesielt for anskaffelsen av *prosjekthotell,* men også sikkerhetssvakhetene som ble påvist i *saksbehandlingsverktøy beboerparkering*.

5. Vil byråden vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?

Svar: Jeg merker meg at anskaffelsene *kontrollverktøy parkering* og *saksbehandlingsverktøy beboerparkering* i stor grad har blitt gjennomført i henhold til regelverk og relevante krav. Da disse anskaffelsene er gjennomført på en tilfredsstillende måte, ser jeg ikke behov for å iverksette tiltak. Jeg vil imidlertid følge opp konklusjonene og anbefalingene i den formelle styringsdialogen med Bymiljøetaten i 2019. Dette gjelder spesielt konklusjonene som framkommer i undersøkelsen av *prosjekthotell*, men også sikkerhetssvakhetene som ble påvist i *saksbehandlingsverktøy beboerparkering* (jf. ovenfor).

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?

Svar: Det vises til svar på spørsmål 5.

7. Oppfattes rapporten som nyttig for kommunen? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.

Svar: Ja, jeg oppfatter den som nyttig og relevant, jf. ovenfor.

8. Hvordan vurderes rapportens oppbygning og språkbruk?

Svar: Rapporten er bygget opp på en ryddig måte og gir leseren en god innsikt i arbeidet og konklusjonene. Rapporten er godt skrevet.

Jeg takker Kommunerevisjonen for en god rapport.

Med hilsen

Lan Marie Berg
byråd

***Godkjent elektronisk***

Oslo kommune
**Byrådsavdeling for oppvekst og kunnskap**

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Dato: 14.12.2018

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| | 201802613-28 | Linda Heen, 23 46 10 97 | 126 |

**RAPPORT TIL UTTALELSE - FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Kommunerevisjonen ber om min uttalelse til rapport fra forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser. Jeg sender her svar på de spørsmål som Kommunerevisjonen stiller i brev sendt 20. november 2018.

1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?

Svar: Problemstillingen som ble kommunisert ved oppstart var «Stiller kommunen gode og relevante sikkerhetskrav i anskaffelser på IKT-området?». Samtidig er undersøkelsen avgrenset til å i hovedsak vurdere prosesskvalitet, og det er kun i liten grad vurdert kvaliteten på det substansielle innholdet i kravene. Avgrensningen er godt begrunnet, og undersøkelsen av prosesskvaliteten har stor verdi, men hovedproblemstillingen kunne kanskje vært formulert slik at denne avgrensningen kom tydeligere frem i en tidlig fase av undersøkelsen.

2. Har byråden kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?

Svar: Jeg har ingen kommentar til metode, kilder eller data.

3. Har byråden kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?

Svar: Revisjonskriteriene fremstår som relevante.

4. Hva er byrådens samlede vurdering av rapportens konklusjoner og anbefalinger?

Svar: Konklusjonene er relevante og logiske med tanke funnene i undersøkelsen, og anbefalingene er nyttige med tanke på forbedringsarbeid knyttet til informasjonssikkerhet.

5. Vil byråden vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?

**Byrådsavdeling for oppvekst og kunnskap**

Postadresse:
Rådhuset, 0037 Oslo

E-post: postmottak@byr.oslo.kommune.no
Org.nr.: 974 767 597

Svar: Jeg tar funnene i Kommunerevisjonens rapport alvorlig, og vil følge opp undersøkelsen i den formelle styringsdialogen med Utdanningsetaten og Barne- og familieetaten i 2019, for å sikre at anbefalingene vil bli lagt til grunn ved fremtidige anskaffelser. Jeg vil be virksomhetene om å sikre at det finnes rutiner for å gjennomføre risikovurderinger i forkant av ikt-anskaffelser og at det gjennomføres tilstrekkelig testing og kontroll over at sikkerhetskravene er levert før nye løsninger settes i produksjon.

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?

Svar: Se svar på spørsmål 5.

7. Oppfattes rapporten som nyttig for kommunen? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.

Svar: Rapporten med anbefalinger oppleves som nyttig og hjelper oss i forbedringsarbeidet knyttet til informasjonssikkerhet.

8. Hvordan vurderes rapportens oppbygning og språkbruk?

Svar: Rapporten har en oversiktlig struktur og er lett å lese.

Med hilsen

Inga-Marte Thorkoldsen
Byråd for oppvekst og kunnskap

***Godkjent elektronisk***

Oslo kommune
**Utviklings- og kompetanseetaten**

Morten A. Engebretsen
Seniorrådgiver
Avdeling for forvaltningsrevisjon,
Kommunerevisjonen

**Unntatt offentlighet**
Offl 23 tredje ledd

Dato: 05.12.2018

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| 18/00378-83 | 18/877-2 | Espen Flereng, 90155437 | |

**UTTALELSE TIL FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Utviklings- og kompetanseetaten (UKE) har gjennomgått Rapport til uttalelse – Forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser og har følgende tilbakemeldinger.

Det har kommet tydelig frem gjennom hele prosessen hva prosjektets hensikt har vært, både omfang og kriterier.

UKE mener dog at det har vært uheldig for helhetsbildet at det ikke er blitt gjennomført intervjuer av deltagerne i de ulike anskaffelsene, sammen med informasjonsinnhentingen. Intervju av sentrale personer i anskaffelsene ville kunne bidratt med en bedre forståelse av prosessene og aktivitetene som er gjennomført. Flere av anskaffelsene ligger noe tilbake i tid og det har vært utfordrende å finne arbeidsdokumentene. I tillegg har kartleggingsarbeidet internt vist at flere av vurderingene som er gjort ikke er tilstrekkelig dokumentert.

I forbindelse med oversending av informasjon 28.5.18, ble kontraktsstrategiene for alle anskaffelsene vedlagt. Kontraktsstrategien blir etablert i planleggingsfasen av anskaffelsen, og før etablering av kravspesifikasjonen. Strategien inneholder konkrete områder man skal ta stilling til i planlegging av en anskaffelse, og oppsummerer resultatet av disse. Et av disse områdene er risikovurdering. For alle tre anskaffelser er det i strategien dokumentert en eller flere risikoer tilknyttet sikkerhet, med tilhørende forslag til tiltak. Disse tiltakene har senere ligget til grunn for utarbeidelsen av sikkerhetskravene i kravspesifikasjonen. UKE mener at dette ikke kommer frem av Kommunerevisjonens vurdering.

UKE mener også at Kommunerevisjonens vurdering av at det i varierende grad fremkommer beskyttelsesbehov for dataene som systemene skal behandle er unyansert. For HMSREG og SMV er det gjennomført verdikartlegging hvor dataenes beskyttelsesbehov for konfidensialitet, integritet og tilgjengelighet er vurdert og dokumentert.

**Utviklings- og kompetanseetaten**

UKE ønsker også å presisere at det ved anskaffelsene SMV og HMSREG er avgitt egen informasjonssikkerhetsressurs (20 %) gjennom anskaffelsesprosjektene.

UKE har ingen kommentarer til revisjonskriteriene.

UKE tar til etterretning at Kommunerevisjonen legger til grunn en større forventning til dokumentering av anskaffelsesprosessen, uavhengig av systemets kritikalitet, enn det UKE har lagt til grunn. Dette gjør at totalvurderingen fremstår som noe ubalansert.

Utover ovennevnte har ikke UKE noen kommentarer til rapportens konklusjoner og anbefalinger.

UKE vil på bakgrunn av rapportens konklusjoner iverksette følgende tiltak:

1. Retningslinjer for anskaffelser er etablert i UKE's styringssystem for informasjonssikkerhet, for å sikre at tilstrekkelige krav til sikkerhet i IKT-anskaffelser er satt, forankret og kommunisert i organisasjonen.
2. UKE planlegger å legge inn oppdatert veiledningstekst i malen for kontraktsstrategien i Veileder for anskaffelser i Oslo kommune, hvor kravene til ivaretakelse og dokumentasjon av informasjonssikkerheten i IKT-anskaffelser kommer tydeligere frem.

Begge tiltakene er planlagt gjennomført i løpet av Q1 2019.

Med hilsen

Marit Forseth
etatsdirektør

Henriette Dan Solberg
avdelingsdirektør

Oslo kommune
**Helseetaten**
Fagsystemavdelingen

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Dato: 27.11.2018

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| 18/00378-82 | 201800770-6 | Ingun Andersen, 97088170 | 126.2 |

**RAPPORT TIL UTTALELSE - FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Det vises til Kommunerevisjonens brav datert 20.11.2018. Kommunerevisjonen har i dette brevet spørsmål som ønskes besvart av Helseetaten. Spørsmål med svar fremkommer nedenfor.

1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?

   *Helseetatens svar:* Ja

2. Har Helseetaten kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?

   *Helseetatens svar:* Ingen kommentarer

3. Har Helseetaten kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?

   *Helseetatens svar:* Ingen kommentarer

4. Hva er Helseetatens samlede vurdering av rapportens konklusjoner og anbefalinger?

   *Helseetatens svar:*
   Rapporten gir et riktig bilde av krav til informasjonssikkerhet i de anskaffelsene som er vurdert.

5. Vil Helseetaten vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?

   *Helseetatens svar:*
   Helseetaten vil i større grad vektlegge risikovurderinger før utarbeidelse av krav til informasjonssikkerhet. Risikovurderinger vil sees i sammenheng med

**Helseetaten**
Fagsystemavdelingen
Besoksadresse:
Storgata 51

Postadresse:
Postboks 4716
0506 OSLO
E-post:
postmottak@hel.oslo.kommune.no

Telefon: 02 180
Telefaks: 23 48 70 70
www.hel.oslo.kommune.no

Bankgiro: 1315 01 01659
Org.nr: 997 506 499

personvernkonsekvensutredninger.

Helseetaten vil i større grad dokumenter hvilke vurderinger som er gjort i forhold til sikkerhetstesting før nye systemer produksjonsettes.

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltakene?

   *Helseetatens svar:*
   Tiltakene iverksettes i tidligfasen i pågående og kommende anskaffelser med tiltaksoppstart primo januar 2019

7. Oppfattes rapporten som nyttig for Helseetaten? Oppgi begrunnelse hvis dette ikke allerede har fremkommet som svar på ovenstående spørsmål.

   *Helseetatens svar:*
   Ja, revisjoner fra Kommunerevisjonen er velkomment. Det gir Helseetaten anledning til stadig forbedring og sørger for at vi måles mot lover, forskrifter og regler som gjelder for offentlig forvaltning og Oslo Kommune.

8. Hvordan vurderes rapportens oppbygning og språkbruk

   *Helseetatens svar:*
   God klar og konsis.

Med hilsen

Runar Nygård
etatsdirektør

Richard Åstrand
avdelingsdirektør

2

Oslo kommune
**Bymiljøetaten**

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Dato: 05.12.2018

Deres ref.: 18/00378-81 Vår ref.: 18/10669-6 Saksbeh.: Magnus Georgsen
Org. enhet: Ressurs- og forvaltningsenheten
Arkivkode: 126

**RAPPORT TIL UTTALELSE – FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER SENDT FRA KOMMUNEREVISJONEN**

Bymiljøetaten viser til oversendt rapport til uttalelse fra forvaltningsrevisjonsprosjektet *Sikkerhetskrav i IKT-anskaffelser*, av 20.11.2018, hvor Kommunerevisjonen ber om skriftlige kommentarer til rapporten innen 06.12.2018, samt svar på åtte spørsmål.

1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?

   Informasjonen om prosjektets hensikt har etter Bymiljøetatens oppfatning vært tilstrekkelig klar.

2. Har Bymiljøetaten kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?

   Bymiljøetaten har ingen kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner.

3. Har Bymiljøetaten kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?

   Etaten har ingen kommentarer til revisjonskriteriene som ligger til grunn for Kommunerevisjonens konklusjoner.

4. Hva er Bymiljøetatens samlede vurdering av rapportens konklusjoner og anbefalinger?

   Bymiljøetaten finner at rapportens overordnede konklusjoner er korrekte ut fra den oversendte dokumentasjonen fra etaten. Kommunerevisjonens anbefalinger vil være nyttige i det videre strategiarbeidet innen anskaffelsesområdet generelt, og for IKT-anskaffelser spesielt.

   I de tre anskaffelsene som Kommunerevisjonen har gjennomgått ser Bymiljøetaten at vår praksis kunne vært mer konsistent, og det har dermed vært nyttig med en gjennomgang som

**Bymiljøetaten**
Postadresse: Postboks 636, Løren 0507 Oslo
Besøksadresse: Karvesvingen 3 0579 OSLO
Telefon: 21 80 21 80 Org.nr: NO 996 922 766
Bankgiro: 1315.01.03376
E-post: postmottak@bym.oslo.kommune.no
Internett: www.oslo.kommune.no

Kommunerevisjonen har gjort. Som en oppfølging av rapporten vil Bymiljøetaten gjøre en gjennomgang av rutiner og prosesser for å sikre konsistens i fremtidige anskaffelser. Etaten har fokus på informasjonssikkerhet, og videre arbeid på dette området blir dermed en etablert som en forbedringsprosess.

5. Vil Bymiljøetaten vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?

   Med bakgrunn i rapportens funn og anbefalinger vil Bymiljøetaten vurdere relevante tiltak. Tiltakene vil konkretiseres nærmere i en plan som lages hvor etaten vil se hen til rapporten. Foreløpig vurderer Bymiljøetaten det som hensiktsmessig å foreta justeringer som ivaretar de forhold som rapporten peker på vedrørende behov når det gjelder rutiner for involvering og samarbeid på tvers av fagmiljøer ved anskaffelser av IKT-relaterte varer og tjenester. Det kan nevnes at Bymiljøetaten har satt i gang et arbeid for å utvikle en ny anskaffelsesstrategi, som også vil berøre forhold vedrørende kontraktsoppfølging og internkontroll. Rapportens funn vil bli vurdert også i denne prosessen.

   Bymiljøetaten vil påpeke at de sikkerhetssvakhetene som er omtalt på siden 6 i rapporten nå er utkvittert, noe som også fremgår i dokumentasjonen som er oversendt Kommunerevisjonen.

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?

   Tiltakene vil iverksettes og gjennomføres i løpet av første halvdel av 2019, når den pågående strategiprosessen for anskaffelsesområdet er fullført (se også kommentarer til spørsmål 5).

7. Oppfattes rapporten som nyttig for Bymiljøetaten? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.

   Rapporten oppfattes som nyttig for etaten. Den bidrar til å kaste lys over viktige momenter som etaten vil ta med seg videre inn i arbeidet med interne prosesser og aktiviteter knyttet til anskaffelser generelt og IKT-anskaffelser spesielt.

8. Hvordan vurderes rapportens oppbygning og språkbruk?

   Rapporten oppbygning og språkbruk er etter Bymiljøetatens oppfatning både lettfattelig og pedagogisk. Og språkbruken vurderes god.

Med vennlig hilsen

Gerd Robsahm Kjørven
etatsdirektør
**Godkjent elektronisk**

Hans Horndalsveen
divisjonsdirektør

Kopi til: Byrådsavdeling for miljø og samferdsel

Oslo kommune
**Barne- og familieetaten**
Administrasjonen

Kommunerevisjonen

Fredrik Selmers vei 3
0663 OSLO

**Unntatt offentlighet**
Offl § 5

Dato: 05.12.2018

| Deres referanse: | Vår referanse.: | Saksbehandler: | Arkivkode: |
|---|---|---|---|
| 18/00378-79 | 18/00621-23 | Frode Karlsvik | 120 |

**DOKUMENT 18/00378-79 TILBAKEMELDING PÅ RAPPORT TIL UTTALELSE – FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Vi takker for mottatt rapport til uttalelse vedrørende forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser.

**Etatens vurdering av rapporten, dens konklusjoner og anbefalinger**

1. Har informasjon om prosjektets hensikt vært tilstrekkelig klar?
   - Ja
2. Har Barne- og familieetaten kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?
   - Ja, angitt nedenfor;

   Kommentar til kapittel 5.2.1 - Avsnitt: Evaluering av tilbyders tilbakemelding på krav til informasjonssikkerhet

   Gjennomgang av Normen sjekkliste som inneholdt mer enn 200 punkter er gjennomført i flere møter høsten 2017 hvor leverandør Visma og intern driftsleverandør UKE i Oslo kommune har stilt med fagkompetanse med hensyn til å gi detaljert og helhetlig beskrivelse av sikkerhetsløsningene av systemet. Oppfyllelse av sikkerhetskrav er detaljert gjennomgått og evaluert i disse møtene, og hvert enkelt punkt er verifisert av personell med nødvendig fagkompetanse.
   I rapport til uttalelse kan det synes som om revisjonen har fått forståelse av at gjennomgang av Normen sjekklisten ble utført i ett møte 08.09.2017, noe som vil gi et noe feilaktig bilde av omfang og detaljnivå av evaluering av krav til informasjonssikkerhet i anskaffelsen. Dokumentasjon av de sikkerhetsmessige løsningene kunne dog vært bedre.

3. Har Barne- og familieetaten kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?
   - Nei
4. Hva er Barne- og familieetatens samlede vurdering av rapportens konklusjoner og anbefalinger?

**Barne- og familieetaten**
Administrasjonen

Postadresse:
Postboks 6726 St. Olavs plass
0130 OSLO
Besøksadresse:

Telefon: 21 80 21 80
Telefax:

Bankkonto: 1315.01.01721
Org.nr.: 976 819 896

E-post: postmottak@bfe.oslo.kommune.no

- Jamfør vår kommentar til punkt 2. Utover dette er vår samlede vurdering at rapportens konklusjoner og anbefalinger gir grunnlag for viktige forbedringsfaktorer for å sikre ivaretakelse av informasjonssikkerhet i IKT-anskaffelser ved Barne- og familieetaten.

5. Vil Barne- og familieetaten vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?
    - Ja, Barne- og familieetaten vil sikre at det gjennomføres ROS-analyse før gjennomføring av anskaffelse, samt forbedre evaluering og testing av sikkerhetskrav ved fremtidige IKT-anskaffelser. Barne- og familieetaten vil vurdere å gjennomføre ny sikkerhetstesting av den aktuelle anskaffelsen.
6. Hvilke tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?
    - Forbedring i forhold til å sikre ivaretakelse av informasjonssikkerhet ved fremtidige IKT-anskaffelser implementeres umiddelbart. Vurdering av ny sikkerhetstesting av den aktuelle anskaffelsen planlegges utført første halvår 2019.
7. Oppfattes rapporten som nyttig for Barne- og familieetaten? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.
    - Ja, rapporten er svært nyttig og gir grunnlag til forbedring for Barne- og familieetaten.
8. Hvordan vurderes rapportens oppbygning og språkbruk?
    - Rapportens oppbygning og språkbruk vurderes å være oversiktlig og lettlest.

Med hilsen

Hege Hovland Malterud
Direktør

Bjørn Arild Lund
Avdelingsdirektør

*Godkjent for elektronisk signatur.*

Oslo kommune
**Utdanningsetaten**

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

**Unntatt offentlighet**
Offl. § 14 . ledd

Dato: 05.12.2018

| Deres ref.: | Vår ref. (saksnr.): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| 18/00378-80 | 18/10156 - 31 | Rohan Fininger | |

**Rapport til uttalelse – Forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser**

Utdanningsetaten viser til brev fra Kommunerevisjonen 20.11.2018 om Forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser. Under følger UDEs tilsvar til Kommunerevisjonens spørsmål:

1. Har informasjonen om prosjektets hensikt vært tilstrekkelig klar?
   UDEs kommentar: Utdanningsetaten finner informasjonen om prosjektets hensikt som tilstrekkelig klar.

2. Har Utdanningsetaten kommentarer til prosjektets metode, anvendte kilder eller data som kan ha betydning for rapportens konklusjoner? I tilfelle hvilke?
   UDEs kommentar: Utdanningsetaten har ingen kommentarer til prosjektets metode, anvendte kilder eller data.

3. Har Utdanningsetaten kommentarer til revisjonskriteriene som ligger til grunn for våre konklusjoner? I tilfelle hvilke?
   UDEs kommentar: Vi er enig med Kommunerevisjonen at det er formålstjenlig å gjennomføre risikovurderinger på informasjonssikkerhetsområdet før kravspesifikasjon utarbeides. Krav til slike risikovurderinger er imidlertid mangelfult beskrevet i Oslo kommunes anskaffelsesveileder.

4. Hva er Utdanningsetatens samlede vurdering av rapportens konklusjoner og anbefalinger?
   UDEs kommentar: Rapporten bidrar til å øke fokuset på informasjonssikkerhet i vår virksomhet.

5. Vil Utdanningsetaten vurdere og eventuelt iverksette tiltak på bakgrunn av rapportens konklusjoner og anbefalinger? I tilfelle hvilke?
   UDEs kommentar: Ja. Etaten har allerede kontaktet Utviklings- og kompetanseetaten for å få oppdatert Oslo kommunes anskaffelsesveileder med krav om at det gjennomføres risikovurderinger av informasjonssikkerhet i forkant av anskaffelser. UDE vil uansett oppdatere egne rutiner for å sikre en ensartet praksis for risikovurderinger før kravspesifikasjoner utarbeides. Tilsvarende vil anskaffelsesrutiner oppdateres med krav om å dokumentere evaluering av oppfyllelse av sikkerhetskravene. Etaten vil også

**Utdanningsetaten**
Besøksadresse: Grensesvingen 6, 0661 OSLO
Postadresse: Postboks 6127 Etterstad, 0602 OSLO
Telefon: 21 80 21 80
postmottak@ude.oslo.kommune.no
www.oslo.kommune.no/skole-og-utdanning/
Org. Nr.: 976820037

oppdatere egne anskaffelsesrutiner for å sikre tilstrekkelig kvalitet på sikkerhetstesting før produksjonstesting.

6. Hvilket tidsperspektiv gjelder for iverksettelse og gjennomføring av tiltak/ene?
   UDEs kommentar: Rutinene som ble beskrevet i punkt 5 vil oppdateres innen første kvartal 2019.

7. Oppfattes rapporten som nyttig for Utdanningsetaten? Oppgi begrunnelse hvis dette ikke allerede har framkommet som svar på ovenstående spørsmål.
   UDEs kommentar: Rapporten oppfattes som nyttig for kommunen og har bidratt til en nyttig kvalitetssikring av det arbeidet etaten gjør på informasjonssikkerhetsområdet.

8. Hvordan vurderes rapportens oppbygning og språkbruk?
   UDEs kommentar: Utdanningsetaten vurderer rapportens oppbygging og språkbruk som god.

Med hilsen

Dag Hovdhaugen
Assisterende direktør

Ian Porter
Assisterende avdelingsdirektør

**Dokumentet er elektronisk godkjent**

Oslo kommune
**Bydel Alna**
Bydelsadministrasjonen

Kommunerevisjonen
Fredrik Selmers vei 3
0663 OSLO

Dato: 27.11.2018

| Deres ref: | Vår ref (saksnr): | Saksbeh: | Arkivkode: |
|---|---|---|---|
| | 201800772-11 | Aina Johansen, 900 26 301 | 126 |

**RAPPORT TIL UTTALELSE - FORVALTNINGSREVISJON AV SIKKERHETSKRAV I IKT-ANSKAFFELSER**

Det vises til rapporten Forvaltningsrevisjon av sikkerhetskrav i IKT-anskaffelser.
Bydel Alna besvarer Kommunerevisjonens spørsmål punkt for punkt:

1. Ja, revisjonen har vært helt tydelige på prosjektets hensikt.

2. Vi har ingen kommentarer til prosjektets metode.

3. Vi har ingen kommentarer til revisjonskriteriene som ligger til grunn.

4. Bydel Alna vurderer rapportens konklusjoner som korrekte. Vi erkjenner at bydelens prosedyrer for anskaffelse av IKT-systemer er brutt, og at vurdering av informasjonssikkerheten ikke er gjennomført.
   Vi vil allikevel bemerke at det er lite sannsynlig at vi ville kommet i samme situasjon igjen, da informasjonssikkerhet og personvern har hatt svært høy prioritet i 2018. Det arbeides nå med å få satt blant annet kontrollfunksjoner i system i bydelens årshjul for informasjonssikkerhet.
   Når det gjelder anbefalinger, se punkt 5.

5. Bydel Alna tar kommunerevisjonens anbefalinger til etterretning, og har allerede satt i gang tiltak i samsvar med disse:
   - Vi har en prosedyre som krever at alle anskaffelser av IKT-systemer skal gå via IKT-seksjonen i administrasjonen. Denne prosedyren må tydeliggjøres overfor bydelens ledere.
   - Vi har opprettet ISK-koordinatorer (informasjonssikkerhetskoordinatorer). Disse (2) samarbeider tett med IKT-koordinator, og vil i samarbeid stille de nødvendige risikobaserte krav til informasjonssikkerhet, ved anskaffelse av nye IKT-systemer med påfølgende testing og kontroll før drift.
   - Vi har utpekt en kontaktperson for personvernområdet, som også er ISK-koordinator. Vedkommende har allerede deltatt i ROS-analyser av andre IKT-systemer, og ser nå også nærmere på de systemene som er gjennomgått i denne revisjonen.
   - Det er gjennomført møter med alle enheter for gjennomgang av systemer etc. i

**Bydel Alna**
Bydelsadministrasjonen

Postadresse:
Postboks 116, Furuset
Trygve Lies plass 1
1001 Oslo
e-post: postmottak@bal.oslo.kommune.no

Telefon: 02 180

Bankkonto: 1315 01 00776
Org nr. 970 534 644

www.oslo.kommune.no

forbindelse med behandlingsoversikten. Her har det vært fokus på ny personvernlov spesielt, men dette har også gitt delvis ivaretakelse av informasjonssikkerhet generelt.
- Det jobbes nå systematisk med å definere roller og få satt kontrollfunksjoner innen informasjonssikkerhetsområdet i system i bydelens årshjul.
- Vi har opprettet en stilling som rådgiver/controller, for tettere kontroll og oppfølging av hele anskaffelsesområdet. Denne stillingen har vært utlyst to ganger uten å bli besatt, så her må vi inntil videre benytte de ressursene vi allerede har innenfor anskaffelser og informasjonssikkerhet.

6. Bydel Alna er allerede godt i gang med gjennomføring av tiltakene.

7. Bydel Alna går i liten grad til anskaffelse av egne systemer. De fleste IKT-systemer i bruk hos oss er anskaffet som sektorsystemer – via UKE eller Helseetaten.
   I arbeidet med å besvare kommunerevisjonens spørsmål til forvaltningsrevisjonen har vi konkludert med at vår kontroll av egne systemer har vært for dårlig, og at det må settes inn tiltak her. Vi må unngå å komme i samme situasjon igjen, hvor systemer blir innkjøpt utenom alle bydelens prosedyrer og retningslinjer.
   Rapporten sier oss altså ikke noe nytt, men prosessen som sådan har vært nyttig og har tydeliggjort svakheter og gitt innspill til videre arbeid.

8. Rapporten har en systematisk og god oppbygning.

Med hilsen

Marius Trana
bydelsdirektør

Solveig Sommer Holm
assisterende bydelsdirektør

Dokumentet er elektronisk godkjent

Oslo kommune
**Kommunerevisjonen**

Grenseveien 88, 0663 OSLO
Telefonnummer: 23 48 68 00
Telefaksnummer: 23 48 68 01

www.krv.oslo.kommune.no
postmottak@krv.oslo.kommune.no

Grafisk produksjon: Allkopi AS - 01.19