Oslo kommune
Kommunerevisjonen

Rapport 05/2014

Intern kontroll i og rundt enkelte IT-systemer - Samlerapport 2013

2014

Kommunerevisjonen - integritet og verdiskaping

Tidligere publikasjoner fra Kommunerevisjonen i Oslo

Rapport 01/2013 Internkontroll med anskaffelsesområdet i Ruter AS
Rapport 02/2013 Internkontroll i- og rundt enkelte IT-systemer. Samlerapport 2012
Rapport 03/2013 Ulike undersøkelser i regnskapsrevisjonen. Samlerapport 2012
Rapport 04/2013 Barneverntjenestenes håndtering av meldinger fra Oslo Krisesenter i 2011
Rapport 05/2013 Informasjonssikkerhet i Vann- og avløpsetaten (unntatt offentlighet)
Rapport 06/2013 Eierskapskontroll i Kollektivtransport-produksjon AS 2010-2012
Rapport 07/2013 Oslo kommunes saksbehandling i Lindebergsakene
Rapport 08/2013 Eierskapskontroll i Oslo Vognselskap AS 2010-2012
Rapport 09/2013 Oslo kommunes oppfølging av berørte etter 22.07.2011
Rapport 10/2013 Sosialtjenestens forvaltning av klientmidler
Rapport 11/2013 Kvalitet i barnehage - Jettegryta barnehage i Bydel Søndre Nordstrand
Rapport 12/2013 Bydelsutvalgenes tilsyn - forståelse, organisering og rapportering
Rapport 13/2013 Bymiljøetatens kontroll og oppfølging av veinettet
Rapport 14/2013 Ivaretakelse av miljøkrav til nye barnehage- og skolebygg
Rapport 15/2013 Anskaffelser i Undervisningsbygg Oslo KF
Rapport 16/2013 Forvaltning av utplasserte kunstverk
Rapport 17/2013 Standpunktkarakterer i videregående skole – likebehandles elevene?
Rapport 18/2013 Eierskapskontroll i Oslo Vei AS
Rapport 01/2014 Behandling av søknader om sykehjemsplass - Bydel Sagene og Bydel Vestre Aker
Rapport 02/2014 Saksbehandlingstid i pedagogisk-psykologisk tjeneste
Rapport 03/2014 Ulike undersøkelser i regnskapsrevisjonen - Samlerapport 2013
Rapport 04/2014 Kommunale boliger - forebygging av utkastelser

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

Forord

God kommunal revisjonsskikk som inkluderer internasjonale revisjonsstandarder angir de ytre rammene for regnskapsrevisjon. Standardene krever planlegging og utførelse av revisjonen på en måte som gir betryggende sikkerhet for at årsregnskapet ikke inneholder vesentlig feilinformasjon. Dette omfatter nødvendig revisjon av IT-systemer som har betydning for økonomi og regnskap.

10. mars 2014

Unn H Aarvold
kommunerevisor

Jan G. Thoresen
seniorrådgiver

Innhold

1. Innledning

Dette er en samlerapport med resultatet av IT-revisjoner og undersøkelser fra siste halvdel av 2012 og hele 2013 og som ikke er presentert for kontrollutvalget tidligere. Detaljene fra undersøkelsene er rapportert til de respektive virksomheter/byrådsavdelinger.

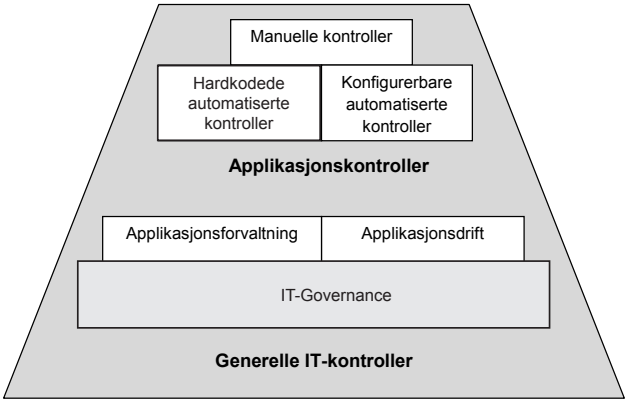
1.1 Tilnærming og metode

Kommunerevisjonens revisjonsmetode bygger på kontrollrammeverket CobiT 4.1. Rammeverket omfatter prosesser og kontroller som er vektlagt i anerkjente kvalitetsstandarder for IT, og som også kommunens styrende IT-dokumenter setter krav til.

Revisjonsobjektene for 2013 er prioritert ut fra en vesentlighetsvurdering av de systemene som behandler økonomiske data. Transaksjonsvolumer og implementering av nye systemer er faktorer som sterkest påvirker prioriteringene, men på særskilte områder kan tidsspennet siden siste gjennomgang også være avgjørende. Kommunen sine fellessystemer er høyt prioritert.

Når nye økonomisystemer er implementert kartlegges transaksjonsflyt og internkontroll i og rundt systemet. Kommunerevisjonen fokuserer på kontroller som fanger opp de største iboende risikoene. Dette er nøkkelkontroller i form av applikasjonskontroller og systemspesifikke generelle kontroller som blir revidert ifølge rotasjonsplaner. Visse nøkkelkontroller er avhengige av saldotabeller, systemrapporter eller automatiserte kontroller. Revisjonen kan også omfatte å teste integriteten i slik funksjonalitet.

Figur 1. Kommunerevisjonen sin internkontrollmodell



Generelle IT-kontroller danner grunnlaget for at IT-systemet skal være velfungerende på lang sikt og støtte opp om virksomhetens mål på det området IT-systemet benyttes. Applikasjonskontroller er maskinelle og manuelle kontroller i og rundt systemfunksjonene som skal sikre fullstendighet, nøyaktighet, gyldighet og sporbarhet i behandlingen av økonomiske transaksjoner.

1.2 Om revisjonene

Kommunens fellessystemer brukes av alle virksomheter i Oslo kommune og er å anse som virksomhetskritiske. Resultatene fra Kommunerevisjonens gjennomgang av Agresso HR blir beskrevet i kapittel to. Systemet har vært gjennom sitt første år i full produksjon og Kommunerevisjonen har særskilt kartlagt og testet viktige sider av tilgangskontrollen. Kommunerevisjonen har også testet integriteten i lønnsrapport for ledere, tvungen arbeidsdeling i selvbetjeningsmodulen og diverse varslinger og spørringer under registrering av lønns- og personaldata.

Kapittel tre beskriver resultatet av en gjennomgang av prioriterte kontroller i Agresso økonomi.

Kapittel fire omhandler arbeidsplansystemet GAT i Oslo kommune. Dette er en undersøkelse som både dekker rutiner for bruk av systemet i virksomhetene og intern kontroll i og rundt de systemfunksjoner som genererer transaksjoner for faste turnustillegg, variabel lønn og fravær til Agresso HR.

Familia er fagsystemet for saksbehandling av barnevernssaker i bydelene og barnevernsvakten i Oslo kommune, herunder vedtak om utbetalinger. Direkte remittering gjelder overføring av vedtatte beløp til privatpersoner v.h.a. nettbankapplikasjonen DnB Connect. Kapittel fem oppsummerer resultatene fra en gjennomgang av remitteringsrutinene i tre bydeler og i tillegg en evaluering av tilgangene til alle bydelenes barnevernskonti i Den Norske Bank.

2. Revisjoner i Agresso HR

2.1 Bakgrunn og formål

Agresso HR er kommunens felles lønnssystem og genererer lønn for ca. 19 milliarder kroner og håndterer i tillegg ca. en milliard kroner i refusjoner fra NAV. Systemet ble fullt ut tatt i bruk november 2012 og har tidligere vært gjenstand for revisjon i begrenset grad.

Formålet med gjennomgangen har vært å undersøke om hensiktsmessige nøkkelkontroller er på plass og fungerer effektivt og å innhente rimelig sikkerhet for at Agresso HR inneholder tilfredsstillende intern kontroll.

2.2 Hovedkonklusjon og sammendrag

Passordrutiner og -regler
Brukeridentifikasjonen i HR-Systemet blir etablert i applikasjonen person- og ressurskatalogen (PRK), men tildeling av tilgang og roller skjer i HR-systemet. Bytte av passord må skje i PRK som synkroniserer dette til Active Directory (AD)[1].

Det ble i 2013 iverksatt et prosjekt som skal sørge for at AD og PRK får to-veis synkronisering, noe som innebærer at passordbytte kan bli mulig på "tradisjonelt" vis.

Rimelighetskontroll av lønn
Kontroll av Lønnsrapport for ledere er en viktig gyldighetskontroll av lønnsutgiftene. Kommunerevisjonen har derfor testet integriteten i denne rapporten.

Kontrollen avdekket at enkelte lønnsutgifter ikke kom med på Lønnsrapport for ledere. Årsaken til dette var at systemet tillot en registreringsvariant som medførte at lønnsutgiften ikke kom med på Lønnsrapport for ledere.

Etter Kommunerevisjonens funn er denne spørringen endret slik at den nå vil fange opp alle lønnsutgifter som er registrert på en slik måte at de ikke kommer med på Lønnsrapport for ledere. Utviklings- og kompetanseetaten har orientert virksomhetene om endringen.

Selvbetjeningsløsningen
Kommunerevisjonen tok høsten 2013 opp svakheter i oppsettet for arbeidsdeling i selvbetjeningsmodulen for variabel lønn. HR-Prosjektet har meldt tilbake at løsningen er endret slik at endringer ikke kan utføres av leder og budsjettansvarlig, at rutinehåndboken er oppdatert og at virksomhetene er informert.

Kommunerevisjonen er informert om at endringene ble implementert i produksjonsmiljøet i januar 2014.

Test av diverse applikasjonskontroller
Noe av bakgrunnen for testene var ett tilfelle av urimelig høy lønnsutbetaling i en bydel. Formålet med testingen var å verifisere om kontroller var etablert og innhente rimelig sikkerhet for at de fungerte hensiktsmessig.

Lønnsprosjektet opplyste at det etter hendelsen ble implementert følgende grensekontroller:

1. Advarsel ved registrering av variabel lønn over et gitt antall timer
2. Transaksjonsstopp ved registrering av variabel lønn over tillatte antall timer
3. Automatisk varsling til remitteringsteamet for utbetalinger over en gitt sum
4. Automatisk varsling til HR-forvaltning ved to eller fler forekomster av samme lønnskonto.

To av kontrollene var implementert da Kommunerevisjonen foretok sine undersøkelser, og det ble under revisjonen ikke avdekket forhold som indikerte at kontrollene ikke fungerte hensiktsmessig. To av kontrollene

[1] Tjeneste som er utviklet av Microsoft for å administrere ressurser

ble ikke revidert da de ikke var aktivisert på undersøkelsestidspunktet.

Tilgangsstyring
Undersøkelsen omfattet ikke autorisasjonsrutiner og annen lokal intern kontroll. Kommunerevisjonen har prioritert områder hvor feilaktige tilganger kan medføre risiko i kommunens regnskaper. Følgende områder er gjennomgått:

- Entydig brukeridentifikasjon
- Omfang av privilegerte brukere
- Omfang av upersonlige brukere
- Enhetlig brukeradministrasjon
- Identitetsstyring
- Arbeidsdeling

Kommunerevisjonens kontroller har i all hovedsak ikke avdekket vesentlige avvik. Det ble observert svak arbeidsdeling i beskjedent omfang.

2.3 Kommunikasjon

Avvik er rapportert løpende til Utviklings- og kompetanseetaten som har respondert løpende. I tillegg er det sendt en informerende oppsummering av revisjonen til Byrådsavdeling for finans 11.02.2014.

3. Revisjoner i Agresso økonomi

3.1 Formål

Formålet med revisjonen har vært å bidra til effektiv regnskapsrevisjon gjennom å vurdere om integriteten i Oslo kommunes felles økonomisystem ivaretar målsettingene om fullstendighet, gyldighet og nøyaktighet i regnskapet.

3.2 Hovedkonklusjoner og sammendrag

Avstemming mellom lønns- og regnskapssystem
Kommunerevisjonen har på stikkprøvebasis kontrollert den avstemmingen Utviklings- og kompetanseetaten gjennomfører pr. virksomhet for hele kommunen hver måned. Det er ikke avdekket feil eller mangler.

Pliktig regnskapsrapportering
Den pliktige regnskapsrapporteringen skjer gjennom forhåndsdefinerte rapporter basert på saldotabeller som genereres ut fra transaksjonene i hovedboken. Kommunerevisjonens tester av integriteten i disse rapportene har ikke avdekket feil eller mangler.

Det er etablert en avstemmingsrapport over summer i viktige saldotabeller mot tilsvarende summering av transaksjoner i hovedboken. Denne rapporten har vært deaktivert i 2013. Rapporten er igjen blitt aktivert etter at Kommunerevisjonen gjorde oppmerksom på dette, og er nå kjørt for alle periodene i 2013. Kommunerevisjonens tester viser at selve rapporten ser ut til å fungere som forutsatt.

Tilganger som medfører både utbetalings- og bokføringsfullmakt
Byrådets rundskriv 12/2004, som ble opphevet for et par år siden, omhandlet blant annet kravet om at bokføringstilgang ikke kan kombineres med utbetalingsfullmakt. Slik Kommunerevisjonen har oppfattet det skal regelen inn i et nytt rundskriv da det ikke var meningen å oppheve regelen.

En sammenstilling av ulike bokføringstilganger i økonomisystemet og HR-systemet med utbetalingsfullmakter i DNB har avdekket at det er flere brukere som har en eller flere bokføringstilganger i kombinasjon med utbetalingsfullmakter.

Funnene er tatt opp med Byrådsavdeling for finans i eget brev for å få en tilbakemelding på hva kommunen mener er tilfredsstillende rutiner og praksis.

Arbeidsdeling i den elektroniske fakturabehandlingen
Kommunerevisjonen har ikke avdekket mangelfull arbeidsdeling i behandlingen av leverandørfakturaer.

Triggere
Kommunerevisjonen har testet merverdiavgiftstriggerne for forholdsmessig fradrag og snudd avregning. Resultatet av disse kontrollene er rapportert til Byrådsavdeling for finans 03.02.2014 som en del av undersøkelsene på merverdiavgiftsområdet

Kommunerevisjonen har ikke avdekket feil eller mangler i dokumentasjonen av triggerne, i grunnlaget for fordelingsnøklene eller i de automatiske beregninger som blir foretatt ved bruk av de nye avgiftskodene for snudd avregning.

Etter en sentral oppdatering av fordelingsnøklene for forholdsmessig fradrag i økonomisystemet, fikk alle virksomhetene tilbakestilt sine nøkler til "malverdier". Dette har medført feil beregning av merverdiavgift i en virksomhet.

I avgiftsoppgaven /terminoppgaven for merverdiavgift fremkommer beløpene knyttet til forholdsmessig fordeling korrekt, men merverdiavgiften knyttet til snudd avregning fremkommer ikke.

3.3 Kommunikasjon

Enkelte av de ovennevnte funn er løpende tatt opp med Utviklings- og kompetanseetaten. En informerende oppsummering av revisjonen ble sendt pr. brev til Byrådsavdeling for finans 11.02.2014.

4. Intern kontroll i og rundt applikasjonen GAT

4.1 Bakgrunn og formål

Arbeidsplansystemet GAT skal beregne og levere godkjente transaksjoner for faste turnustillegg, variabel lønn og fravær til HR-systemet. Formålet med undersøkelsen var å oppnå betryggende sikkerhet for at tilfredsstillende intern kontroll var etablert, slik at kommunens regnskaper ikke inneholder vesentlige feil og systemet produserer gyldige og nøyaktige lønnsutgifter. Et annet formål med undersøkelsen var å kartlegge hvordan virksomhetene ved hjelp av GAT fulgte opp Arbeidsmiljølovens arbeidstidsbestemmelser.

4.2 Hovedkonklusjon og sammendrag

Virksomhetenes etterlevelse av gjeldende rutiner for oppfølging og gjennomgang av overføring av timelister til Agresso HR var mangelfull. Dette har medført at opptjent variabellønn i flere tilfeller ikke har blitt utbetalt i tide. Forholdet gjaldt samtlige undersøkte virksomheter.

Omfanget av gamle, ikke overførte timelister var betydelig. I sin tilbakemelding melder virksomhetene at noen av disse timelistene enten var overført manuelt til Agresso HR eller var feilregistrerte timelister. Kommunerevisjonens oppfatning er at i slike tilfeller bør likevel timelistene passiviseres i GAT slik at man får en fullstendig oversikt over ikke overførte og utbetalte timelister.

Kommunerevisjonen har i brev til alle kommunens virksomheter som benytter GAT anbefalt at det foretas en fullstendig gjennomgang av rapport 60 for å sikre at all lønn som skulle ha vært utbetalt er utbetalt. Virksomhetene bør påse at rapport 60 gjennomgås løpende i samsvar med gjeldende veileder for å sikre at lønn blir utbetalt korrekt og rettidig.

Mangler i applikasjonskontrollene knyttet til avstemmingsfunksjonaliteten skaper risiko for at ikke overførte lønnstransaksjoner fra GAT til Agresso HR ikke blir avdekket.

For øvrig ble det avdekket enkelte svakheter i applikasjonskontrollene men disse var kompensert med manuelle rutiner.

Det ble ikke avdekket signifikante avvik i de generelle IT-kontrollene.

4.3 Kommunikasjon

En oppsummering av revisjonen ble sendt til Byrådsavdeling for eldre og sosiale tjenester med kopi til reviderte virksomheter den 28.01.2014. Byrådsavdelingen gav sitt svar 19.02.2014. Byrådsavdeling skriver at de vil følge opp undersøkelsen ved å be Helseetaten å tilby ytterligere opplæring i rutine for fravær og variabel lønn, utarbeide en bedre prosedyre for å tildele førstegangspassord og at dokumentert prosedyre for endringshåndtering av faste, kritiske data er utarbeidet.

5. Direkte remittering fra Familia

5.1 Bakgrunn og formål

Familia er fagsystemet for saksbehandling av barnevernssaker i Oslo kommune, herunder vedtak om utbetalinger. Direkte remittering gjelder overføring av vedtatte beløp direkte til privatpersoner i nettbankapplikasjonen DnB Connect. De månedlige beløpene varierer mellom kr.100.000,- og kr. 200.000,- pr. barnevernskontor.

DnB Connect ble tatt i bruk januar 2012. Familia fikk ny driftsleverandør november 2012 samtidig som Utviklings- og kompetanseetaten overtok en del viktige administrasjons- og serviceoppgaver.

Direkte remittering er ikke revidert tidligere.

Revisjonen omfattet rutiner og kontroller i tre bydeler og en test av tilgangene til alle kommunens barnevernskonti i Den norske Bank.

Revisjonens formål var å innhente rimelig sikkerhet for at direkte remittering fra Familia til DnB Connect ble håndtert på en tilfredsstillende måte som sikrer nøyaktig og korrekt overføring av transaksjoner mellom systemene.

5.2 Hovedkonklusjoner og sammendrag

Etter Kommunerevisjonens vurdering var det i all hovedsak implementert gode internkontroller rundt prosessen for direkte remittering i de tre barnevernskontorene som var gjenstand for revisjon. Rutinehåndboken som er utarbeidet av Helseetaten ble brukt noe ulikt i de tre barnevernskontorene og Kommunerevisjonen konstaterte at ikke alle anbefalte kontroller var implementert, dette relaterte seg spesielt til gjennomgang av tilganger og avvikslogg. Kommunerevisjonen observerte svakheter knyttet til brukeradministrasjon i Familia og i tilganger gitt til Familia og DnB Connect.

5.3 Kommunikasjon

Revisjonsresultatene ble meddelt Byrådsavdeling for eldre og sosiale tjenester og de reviderte bydelene i brev av 25.02.2013.

Byrådsavdelingen meldte tilbake i brev av 25.04.2013 at flere av de forhold som ble avdekket ville medføre endringer i Rutinehåndbok for Familia, og redegjorde mer detaljert for hvordan Kommunerevisjonens anbefalinger ville bli møtt. Byrådsavdelingen planla å meddele resultatet samlet til bydelene når ny rutine for direkteremittering var utarbeidet i forbindelse med at Familia fikk ny IKT driftsplattform på et senere tidspunkt i 2013. Vårt inntrykk var at Byrådsavdelingen hadde en konstruktiv tilnærming til rapportens anbefalinger.

De tre bydelene gav tilbakemeldinger om at Kommunerevisjonens anbefalinger i all hovedsak var fulgt.

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 - 05.14