Oslo kommune
Kommunerevisjonen

Rapport 02/2013

Intern kontroll i og rundt enkelte IT-systemer

Samlerapport 2012

2013

Kommunerevisjonen - integritet og verdiskaping

Tidligere publikasjoner fra Kommunerevisjonen i Oslo

Rapport 01/2012 Gjennomgang av anskaffelsesdokumentasjon i 16 virksomheter
Rapport 02/2012 Bydelene som barnehagemyndighet – Bydel St. Hanshaugen og Bydel Nordstrand
Rapport 03/2012 Styringsinformasjon i Utviklings- og kompetanseetaten
Rapport 04/2012 Utleie av kommunal grunn - saksbehandling, kontroll og oppfølging
Rapport 05/2012 Anskaffelse, kontroll og oppfølging av tjenester til utviklingshemmede – Bydel Frogner og Bydel Nordre Aker
Rapport 06/2012 Planlegging av investeringsprosjekter i Vann- og avløpsetaten
Rapport 07/2012 Ulike undersøkelser i regnskapsrevisjonen – samlerapport 2011
Rapport 08/2012 Skolens saksbehandling knyttet til spesialundervisning – Korsvoll skole, Lindeberg skole, Skøyenåsen skole, Tiurleiken skole
Rapport 09/2012 Intern kontroll i og rundt enkelte IT-systemer – Samlerapport 2011
Rapport 10/2012 Informasjonssikkerhet i Energigjenvinningsetaten
Rapport 11/2012 Informasjon om tannhelsetjenester til mottakere av hjemmesykepleie – Bydel Alna og Bydel Vestre Aker
Rapport 12/2012 Etterlevelse av finansreglementet i Oslo kommune
Rapport 13/2012 Forvaltning av Gerica i Oslo kommune og intern kontroll rundt inntekter fra praktisk bistand
Rapport 14/2012 Sosialtjenestens oppfølging av rusmiddelavhengige ved behandlingsopphold
Rapport 15/2012 Ledelsesforankring av innkjøpsområdet i Sykehjemsetaten
Rapport 16/2012 Kontroll og oppfølging av kvalitet i kommunale institusjoner for rusmiddelavhengige
Rapport 17/2012 Rapportering av statistikk for pleie- og omsorgstjenester
Rapport 18/2012 Ettervern Barneverntiltak for ungdom etter fylte 18 år i Bydel Gamle Oslo og Bydel Stovner
Rapport 19/2012 Registrering av elever i risikosonen for frafall. Bruken av koden "ELEV" i IT-systemet OTTO
Rapport 20/2012 Oppfølgingsundersøkelse etter rapport 18/2009 Sykehjemsetaten – status etter to års drift.
Rapport 21/2012 Tjenester til beboere i samlokaliserte boliger - Bydel Stovner
Rapport 22/2012 Internkontroll i Kollektivtransportproduksjon AS med datterselskaper
Rapport 23/2012 Anskaffelser og internkontroll i Oslo Vognselskap AS
Rapport 01/2013 Internkontroll med anskaffelsesområdet i Ruter AS

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.

13. mars 2013

Unn H. Aarvold
kst. kommunerevisor

Torun Rinnan
senior revisjonsrådgiver

Innhold

Forord **1**

1. Innledning **5**
1.1 Om revisjonene 5

2. Fellestrekk ved revisjonene **7**
2.1 Innledning 7
2.2 Metodikk ved våre revisjoner 8
2.3 Fellestrekk ved revisjonsresultatene 8
2.4 Vurdering av revisjonsresultatene 9

3. Masseremittering fra Agresso til DnB Connect **11**
3.1 Bakgrunn og formål 11
3.2 Hovedkonklusjon og sammendrag 11
3.3 Kommunikasjon 12

4. Drift av kommunens lønnssystem (NLP) **14**
4.1 Bakgrunn og formål 14
4.2 Hovedkonklusjon og sammendrag 14
4.3 Kommunikasjon 14

5. Revisjon av nytt lønnssystem **15**
5.1 Bakgrunn og formål 15
5.2 Hovedkonklusjon og sammendrag 15
5.3 Kommunikasjon 16

6. Diverse revisjon av fellessystemer **17**
6.1 Bakgrunn og formål 17
6.2 Hovedkonklusjon og sammendrag 17
6.3 Kommunikasjon 18

7. Revisjon av FAS og rutiner og kontroller knyttet til inntekter fra alarmabonnementer og unødige utrykninger **19**
7.1 Bakgrunn og formål 19
7.2 Hovedkonklusjon og sammendrag 19
7.3 Kommunikasjon 19

8. Lokal og sentral tilgangsadministrasjon i SATS barnehage **20**
8.1 Bakgrunn og formål 20
8.2 Hovedkonklusjon og sammendrag 20
8.3 Kommunikasjon 20

9. Revisjon av Xpand og husleieinntekter 21
9.1 Bakgrunn og formål 21
9.2 Hovedkonklusjon og sammendrag 21
9.3 Kommunikasjon 21

10. Revisjon av inntekter fra Ungbo via Concorde 22
10.1 Bakgrunn og formål 22
10.2 Hovedkonklusjon og sammendrag 22
10.3 Kommunikasjon 22

11. Revisjon av Picasso og gjennomgang av inntekter ved Øvingshotellet.....23
11.1 Bakgrunn og formål 23
11.2 Hovedkonklusjon og sammendrag 23
11.3 Kommunikasjon 23

12. Generelle it kontroller i PAX, oppfølging av fjorårets revisjon.....24
12.1 Bakgrunn og formål 24
12.2 Konklusjon og sammendrag.....24
12.3 Kommunikasjon 24

1. Innledning

Dette er en samlerapport med resultatet av ti IT-revisjoner og undersøkelser som ble gjennomført i 2012 og som ikke er presentert for kontrollutvalget tidligere.

Formålet med de ulike IT-revisjonene er å gjennomgå og evaluere den interne kontrollen i og rundt IT-systemer av betydning for regnskapet. Målet er å gi en rimelig sikkerhet for at IT-systemene er satt opp på en måte som sikrer korrekt regnskapsrapportering. Resultatene av alle revisjonene og undersøkelsene er i all hovedsak rapportert til de respektive virksomhetene / byrådsavdelingene på et detaljert nivå, og vi har mottatt tilbakemelding om eventuelle tiltak.

Denne rapporten inneholder bakgrunn og konklusjon fra hver av de ti IT- revisjonene og undersøkelsene som er gjennomført. I tillegg presenterer vi en sammenligning av noen av kontrollpunktene som omhandler generelle IT- kontroller fra de ulike revisjonene. Disse er rapportert i et eget avsnitt for å vise fellestrekk, jf. kap 2.

1.1 Om revisjonene

Revisjonene er gjennomført basert på en overordnet risikovurdering som konkluderer på viktigheten av systemet for behandling av økonomiske data for den enkelte virksomhet. Stort transaksjonsvolum, implementering av nye systemer, kompleksitet og mange grensesnitt er faktorer som gir innspill til, og påvirker, vår risikovurdering ved gjennomføring av IT-revisjoner.

DnB erstattet Nordea som kommunens hovedbank fra 1. januar 2012 og DnB Connect er DnB sin nettbank. En av revisjonene omhandler masseremittering fra Agresso til DnB Connect, se kap. 3.

NLP håndterte ca. 65% av lønnskostnadene for Oslo Kommune i 2012. I kapittel 4 gjengis resultatene fra en ekstern revisjon av driftsmiljøet til NLP. Undersøkelsen er gjennomført av driftsleverandørens eksterne revisor og følger en standard som er tilrettelagt for at Kommunerevisjonen kan bygge på revisjonsresultatene.

Agresso HR er i løpet av 2012 rullet ut i alle kommunens virksomheter parallelt med utfasingen av NLP. I kapittel 5 har vi laget en oppsummering av aktiviteter som Kommunerevisjonen har utført for å kunne revidere det nye HR systemet på en mest mulig effektiv måte.

I kapittel 6 gjengis resultatene fra ulike revisjonshandlinger rettet mot fellessystemene i Oslo Kommune der formålet har vært å bidra til en effektiv regnskapsrevisjon.

I kapittel 7 oppsummeres en revisjon av Brann- og redningsetatens alarmhåndteringssystem FAS som benyttes til registrering av alarmabonnement og utrykninger ved 110 - sentralen, herunder kontroller i og rundt grensesnittet til Agresso.

I kapittel 8 presenterer vi funnene fra en revisjon av lokal og sentral tilgangsadministrasjon i SATS barnehage. Systemet benyttes av alle bydeler i forbindelse med registrering av opplysninger relatert til barn i barnehage og beregning av månedlig oppholdsbetaling for disse.

En oppsummering av revisjon av Xpand og husleieinntekter i Omsorgsbygg er presentert i kapittel 9. Xpand er Omsorgsbyggs system for forvaltning, drift og vedlikehold av eiendommer, herunder beregning av husleieinntekter.

Revisjon av Concorde som benyttes av Ungbo i forbindelse med forvaltning av boliger, herunder husleieinntekter, oppsummeres i kapittel 10.

Picasso er et støtteverktøy for kundebehandlere og faktureringsansvarlige, og er et standard bookingsystem for hoteller som er tilpasset Øvingshotellet. Revisjon av Picasso og inntekter hos Øvingshotellet er gjengitt i kapittel 11.

Til slutt, i kapittel 12, gjengir vi en oppfølging av en revisjon gjennomført i 2011 av generelle IT kontroller i PAX. Dette er Kemnerkontorets system for fakturering, regnskapsføring og innkreving av gebyrer for Trafikketaten.

2. Fellestrekk ved revisjonene

2.1 Innledning

Kommunerevisjonen har gjennomgått og gjennomført en sammenligning av noen av kontrollpunktene i seks av de gjennomførte IT-revisjonene i 2012. Dette er generelle IT-kontroller som er felles for flere av kommunens virksomheter. Hensikten er å se på mulige fellestrekk.

Det er de siste par årene også gjennomført flere revisjoner som har avdekket alvorlige svakheter knyttet til informasjonssikkerhet i virksomheter under Byrådsavdeling for miljø og samferdsel.

Formålet med å gjennomføre en sammenligning, uavhengig av virksomhet, er på et generelt grunnlag å kunne gi innspill til områder hvor det kan være svakheter basert på erfaring i andre virksomheter. På denne måten håper vi at både virksomhetene og kommunen sentralt kan bruke resultatene i et lærings- og forbedringsarbeid som kan være viktig for flere enn bare de reviderte virksomhetene.

Oslo kommune jobber med å forbedre seg på IKT-området. I 2011 startet kommunen et informasjonssikkerhetsprosjekt som eies og ledes av Byrådsavdeling for finans. Hensikten med prosjektet er ifølge byrådsavdelingen å utvikle og klargjøre for implementering et hel-hetlig internkontroll- og styringssystem for informasjonssikkerhet med styrende dokumenter på overordnet nivå som en del av det kontinuerlige forbedringsarbeidet.

Som en del av prosjektet foretok kommunen våren 2011 en egenevaluering på ulike områder knyttet til informasjonssikkerhet i alle virksomhetene i kommunen. Egenevalueringen innebar først og fremst en kartlegging av i hvilken grad virksomhetene vurderte at de hadde dokumenterte rutiner og retningslinjer og ikke en direkte måling av den faktiske informasjons-sikkerhetstilstanden i virksomhetene. Egenevalueringen viste veldig tydelig rom for forbedring, spesielt i forhold til bruk av risikovurderinger og dokumentering av gjennomførte tiltak, organisering av roller og ansvar, dokumenterte rutiner for b.la håndtering av hendelser, kontinuitetsplanlegging og etterlevelse.

Ser vi virksomhetenes egenevaluering opp mot de svakhetene vi avdekker under våre gjennomførte IT-revisjoner så kan vi se at det er en sammenheng.

Opprinnelig plan var en avslutning av prosjektet våren 2013. Informasjonssikkerhetsprosjektet er forsinket i forhold til dette. Høsten 2012 vedtok styringsgruppen til prosjektet å inkludere en revisjon av kommunens gjeldende informasjonssikkerhetsinstruks fra 2001 i prosjektet for å sikre en mer overordnet struktur og et klart eierskap til informasjonssikkerheten i kommunen. I tillegg var det ønskelig med en tydeliggjøring av ansvaret som ligger i de ulike rollene på informasjonssikkerhetsområdet. Arbeidet med å få på plass en revidert informasjonssikkerhetsinstruks antas ifølge prosjektet å være ferdig i løpet av våren 2013.

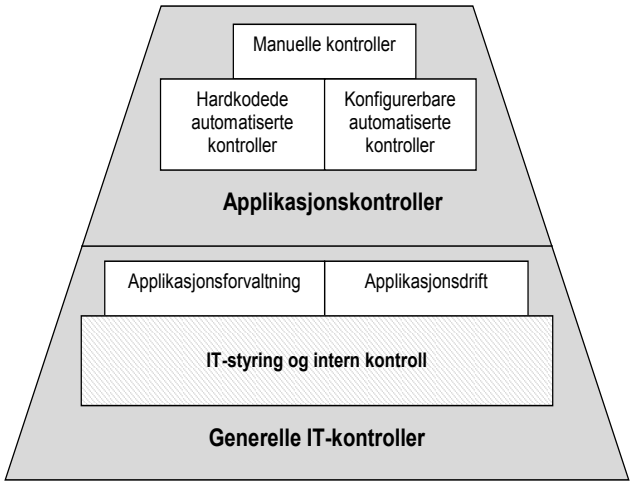
Informasjonssikkerhetsprosjektet har utarbeidet utkast til veiledere og maler, og med basis i disse og instruksen vil Byrådsavdeling for finans utforme endelige rundskriv, veiledere og maler på området. Parallelt med arbeidet med å revidere informasjonssikkerhetsinstruksen er det utarbeidet en utdypende metodikk for risikovurdering som noen virksomheter i kommunen har vært med på å prøve ut. Når informasjonssikkerhetsprosjektet blir ferdig vil kommunen i følge prosjektet ha grunnlag for å utøve god styring og kontroll på informasjonssikkerhetsområdet.

2.2 Metodikk ved våre revisjoner

Generelle IT-kontroller er kontroller man har på IT-området og som ivaretas helt eller delvis av en IT-avdeling. Disse skal være med på å sikre og understøtte fullstendighet, rettidighet, nøyaktighet, pålitelighet og sporbarhet av forretningstransaksjoner.

Vår metode ved IT- revisjoner bygger på CobiT som er et globalt anerkjent rammeverk for styring og kontroll av IT, og omfatter prosesser og kontroller som også finnes i kommunens instruks for informasjonssikkerhet. Internkontrollmodellen som vi reviderer etter er illustrert i Figur 1.

Figur 1.



I rapporteringen som presenteres i kapittel 2.3, har vi tatt utgangspunkt i de viktigste problemstillingene og svakhetene vi har identifisert i våre revisjoner av generelle IT-kontroller i de ulike virksomhetene.

Applikasjonskontroller og IT- avhengige kontroller er avhengig av generelle IT-kontroller for å fungere tilfredsstillende, og av disse er tilgangskontroller og endrings-håndtering, etter Kommunerevisjonens vurdering, å anse som de mest kritiske. Vi har i all hovedsak derfor valgt å fokusere på disse to områdene under revisjonene i 2012.

2.3 Fellestrekk ved revisjons-resultatene

Felles trekk fra revisjonene og vurderings-skalaen kan illustreres som følger:

SKALA:	JA	NEI	NOE	IKKE VURDERT

Kriterium	System 1	System 2	System 3	System 4	System 5	System 6
1. Tilgangskontroller						
1.1 Eksisterer det oppdaterte og skriftlige prosedyrer for hvordan tilgangskontroller skal tildeles, administreres og følges opp?	1	2	2	3	1	3
1.2 Er privilegerte brukere/administratorer begrenset til kun autorisert personell?	1	1	1	1	3	2
1.3 Er tilgangskontroller implementert for å støtte tilfredsstillende arbeidsdeling i kritiske funksjoner i forretningsprosessen	3	3	2	1	3	1
1.4 Blir tilganger til systemet regelmessig gjennomgått?	2	2	2	2	2	1
2. Endringshåndtering						
2.1 Eksisterer det oppdaterte og skriftlige prosedyrer for endrings-håndtering (autorisasjon, dokumentasjon,testing,godkjenning og arbeidsdeling)?	2	2	2	4	4	3
2.2 Gjennomføres endringshåndtering iht. til skriftlige prosedyrer	4	2	2	4	4	3
2.3 Blir endringer som gjennomføres overvåket?	4	2	2	4	4	4

2.4 Vurdering av revisjonsresultatene

Med utgangspunkt i tabellen, har vi evaluert de gjennomgåtte IT-prosessene tilgangskontroller og endringshåndtering og vurdert risikoene som de identifiserte svakhetene representerer for kommunen.

Det er likhetstrekk med resultatet som ble rapportert som fellestrekk i fjor når det gjelder tilgangskontroller og endringshåndtering. Området som omfatter endringshåndtering kommer dårligere ut i forhold til fjorårets rapportering, dette kan også være tilfeldig ut i fra hvilke systemer som er revidert. Det er likevel på det rene at både tilgangskontroller og endrings-håndtering er to områder der det er utfordringer i forhold til rutiner og dokumentasjon.

1. Tilgangskontroller

Gode tilgangskontroller er viktige bl.a. for å forebygge og oppdage misligheter og feil

i regnskapet. Vi har undersøkt dette i seks revisjoner i 2012. Som figuren ovenfor viser er det avdekket en god del svakheter på dette området.

Manglende oppdaterte og skriftlige prosedyrer for hvordan tilganger skal tildeles, administreres og følges opp er en gjennomgående svakhet. Dette gir en økt risiko for at tilgangskontroller ikke blir implementert på en tilfredsstillende måte.

I fem av seks revisjoner finner vi at gjennomgang av tilganger ikke blir utført. Dette gir en økt risiko for uautoriserte tilganger til IT-systemene da eventuelle feil i og for vide tilganger ikke blir oppdaget.

2. Endringshåndtering

En god endringshåndteringsprosess er viktig for å sikre at et IT- system fungerer som forutsatt og bidrar til den måloppnåelsen som IT- systemet er ment å gi. Vi har vurdert endringshåndtering i fire av de seks revisjonene som er illustrert i figuren ovenfor og vi ser at dette er et område med flere svakheter når det gjelder rutiner og dokumentasjon. En uformell endringshåndteringsprosess øker risikoen for uautoriserte endringer og at IT- systemene ikke blir oppdatert med riktig funksjonalitet til riktig tid.

3. Masseremittering fra Agresso til DnB Connect

3.1 Bakgrunn og formål

Oslo Kommune brukte tidligere Nordea som bankforbindelse, men DnB ble valgt som ny hoved leverandør av banktjenester fra og med januar 2012.

DnB stiller nettbankapplikasjonen DnB Connect til rådighet for Oslo kommune som abonnerer på tjenesten. All utvikling av applikasjonen skjer hos DnB.

Revisjonens formål er å innhente rimelig sikkerhet for at regnskapene ikke inneholder vesentlige feil når det gjelder håndtering av masseremittering fra Agresso som følge av svakheter i DnB Connect. Masseremittering er en tjeneste som håndteres av Utviklings- og kompetanseetaten på vegne av alle virksomhetene i Oslo Kommune. Iht. årsberetningen til Utviklings- og kompetanseetaten for 2012, behandlet fakturasentralen ca. 630.000 fakturaer til Oslo kommunes virksomheter i 2012.

3.2 Hovedkonklusjon og sammendrag

Systemforvaltning
Byrådsavdeling for finans skrev et brev til UKE høsten 2011 der de definerte overordnet hvilke arbeidsoppgaver de så for seg at administratorene hos Utviklings- og kompetanseetaten skulle ha knyttet til brukeradministrasjon i DnB Connect. I rutinehåndbokens kap. 6 «administrasjon av brukere, kontoer og divisjoner» er administratorenes oppgaver nærmere definert. Det er i innkjøringsfasen av DnB Connect ikke foretatt noen systematisk oppfølging av at Utviklings- og kompetanseetaten utfører de arbeidsoppgavene de er satt til å håndtere. Vi har avdekket manglende definering og dokumentasjon av arbeidsoppgaver for administratorer og dette øker risikoen for at arbeidsoppgaver ikke blir gjennomført eller at de gjennomføres på feil måte.

Det er ikke etablert en formell prosess for endringshåndtering rundt DnB Connect i Oslo Kommune. Det finnes en uformell rutine for at brukerne kan komme med endringsønsker til Byrådsavdeling for finans. Det avholdes jevnlige driftsmøter mellom banken, Byrådsavdeling for finans, representanter fra Utviklings- og kompetanseetaten og Helseetaten[1] der endringsforslag kan fremlegges, og så er det opp til banken om de ønsker å videreføre ønskene.

Administratorene i UKE er ikke kjent med om det finnes en kanal for å komme med endringsønsker, hverken til Byrådsavdeling for finans eller DnB. Manglende felles rutine for å fange opp, prioritere og å melde endringsønsker øker risikoen for at systemet ikke dekker kommunens behov på en optimal måte. Administratorene i Utviklings- og kompetanseetaten påpeker eksempelvis manglende funksjonalitet for søk og lite brukervennlige tilgangsoversikter i nettbanken.

Tilgangskontroller og arbeidsdeling
Det er etablert tvungen dualkontroll[2] i tilgangsadministrasjonen. Ifølge bruker-håndboka kap. 6.4.2 skal en administrator ikke gis tilgang til konto eller divisjon. Vi har verifisert at administratorer har tilgang til å endre egne rettigheter for divisjoner. Dette har forekommet under administrasjon av sigilleringsparametre[3] der noen har gitt seg selv tilgang til å endre divisjoner.

[1] Helseetaten er fagansvarlig for alle sektor systemene
[2] To personer må være involvert i endringer som foretas.
[3] Agresso har en egen funksjonalitet for sigillering (for-segling av fil). Sigilleringsparameterne i Agresso er sigillgenerator (32 tall) og sekvensteller. Endringer i parameterne uten tilsvarende endringer i Connect vil medføre sigilleringsfeil.

Administratorer har tilgangsprivilegier i både DnB Connect og Agresso og har dermed mulighet til å implementere tilganger som vil representere svak arbeidsdeling og gi en risiko for feil utbetalinger. Tvungen dualkontroll kompenserer delvis for denne risikoen.

Når det gis tilgang i DnB Connect sjekker administratorene tilgangsautorisasjoner opp mot brukernes tilganger i Agresso på eget initiativ for å forhindre brudd på arbeidsdelingsprinsippene. Ved slike konflikter kontakter administrator aktuell autorisasjonsansvarlig. Tilsvarende kontroll utføres imidlertid ikke i Agresso. Administratorene er usikre på hvilket ansvar de har når arbeidsdelingsprinsippene brytes og hvilken myndighet de har til å nekte tilgang ved en konflikt i bestilte/gitte tilganger i DnB Connect. De etterlyser retningslinjer på dette området for å kunne håndtere jobben på en best mulig måte. Det arbeides med å få på plass en rapport som avdekker prinsippbrudd mellom Agresso og DnB Connect og vi anbefaler Byrådsavdeling for finans å etablere rutiner for kontroll av brudd på arbeidsdelingsprinsippene mellom Agresso og nettbanken. Disse kan eksempelvis være en del av rutinene for regelmessig gjennomgang av tilganger i systemene.

Vi har avdekket at åtte personer hadde inkompatible tilganger i DnB Connect og Agresso og som er i strid med kommunens føringer om tilgangskontroller i Rundskriv 12/2004. Risikoen for uautorisert remittering/ utbetaling i nettbanken er delvis kompensert med tvungen arbeidsdeling i DnB Connect.

Oslo kommune har ikke tilstrekkelig tilgang til logger i DnB Connect. Loggen over endringer i tilganger som administratorene har tilgang til, brukes ved behov og er ikke tilrettelagt for regelmessig oppfølging. Byrådsavdeling for finans har stilt krav til loggfunksjonalitet i nettbankløsningen for at det skal være mulig å spore tilbake til ansvarlig bruker ved eventuelle hendelser. I følge Byrådsavdeling for finans er det ikke gjort noen vurdering av behov for og bruken av loggfunksjonalitet i DnB Connect ut over det.

Brukerautorisasjon og gjennomgang av brukere

Byrådsavdeling for finans har utarbeidet hensiktsmessige rutiner for autorisasjon av brukere i nettbanken i Oslo kommune. Autorisasjonsskjemaet er imidlertid utarbeidet av DnB og skjemaet er ikke tilpasset Oslo Kommune sitt behov. Skjemaet er lite brukervennlig, både for de som fyller det ut og administratorene som leser det. Det er ikke utarbeidet noen veiledere for utfylling av skjemaet. Dette representerer en risiko for at skjemaet blir feil utfylt, noe som igjen kan medføre at brukere får tilganger de ikke skulle hatt. I tillegg medfører disse uklarhetene merarbeid for administratorene som må kontakte virksomhetene for å korrigere skjemaene.

Administratorer kontrollerer signaturer på autorisasjonsskjemaer, men de mangler oversikt over personer med autorisasjonsmyndighet. Dette øker risikoen for at brukere får uautorisert tilgang til funksjoner i systemet

Pr. i dag er det ikke etablert rutiner for gjennomgang av tilgangsrettigheter i DNB Connect, hverken i Utviklings- og kompetanseetaten eller i virksomhetene. Lite brukervennlige tilgangsrapporter i nettbanken, manglende tilgang til fullstendige oversikter hos virksomhetene og ikke-søkbare autorisasjonsskjemaer gjør det vanskelig å kontrollere at tilgangene til virksomhetens bankkonti er korrekt implementert.

3.3 Kommunikasjon

Oppsummering av revisjonen ble sendt pr. brev til Byrådsavdeling for finans med kopi til Utviklings- og kompetanseetaten 05.10.2012. Byrådsavdelingen skriver i sitt svarbrev til Kommunerevisjonen at de er enig

i forholdene som påpekes og skal sørge for risikoreduserende tiltak knyttet til de svakheter Kommunerevisjonen har avdekket knyttet til systemforvaltning og tilgangskontroller.

Det fremkommer videre at arbeidet er igangsatt, og i det videre arbeidet vil byrådsavdelingen ha god nytte av de observasjoner og vurdering av risiko som Kommunerevisjonen har gjort.

4. Drift av kommunens lønnssystem (NLP)

4.1 Bakgrunn og formål

Oslo Kommune har i 2012 brukt Evry[4] som driftsleverandør av NLP. NLP behandlet i 2012 vesentlige deler av kommunens lønnsutgifter og refusjonsinntekter. Evry sine aktiviteter er således vesentlige for kommunen og er av betydning for revisjonen.

Kommunerevisjonen reviderer normalt ikke IT-miljøet hos kommunens serviceleverandører. Revisjonen bygger på en uttalelse fra Evry sin revisor, som er Ernst & Young (E&Y). Uttalelsen følger regnskapsstandarden ISAE 3402 – Attestasjonsuttalelser om kontroller hos en serviceorganisasjon.

E&Y er en av de største internasjonale revisjonsselskapene, og har etter vår vurdering tilfredsstillende kompetanse til å utføre denne type oppdrag. E&Y har utarbeidet en uttalelse om utformingen, implementeringen og måleffektiviteten av intern kontroll i Evry sine operasjonelle prosesser. Uttalelsen gjelder for forretningsområdet «løsninger Offentlig» som NLP har sortert under.

Uttalelsen gjelder ledelsens beskrivelse av intern kontrollsystemet, dets design og om det fungerer hensiktsmessig. Sistnevnte er basert på resultatet av testing av et utvalg kontroller. Utvalgsmetoden er en kombinasjon av sampling og skjønnsmessige individuelle risiko-vurderinger. Testfrekvensen kan være årlig, kvartalsvis, månedlig, ukentlig, hendelsesdrevet eller kontinuerlig[5]. For 2012 er utvalgte kontroller testet under følgende områder:

Styre hendelser (4 kontroller – 1 avvik)
Styre problemer(4 kontroller – 3 avvik)
Styre endringer (7 kontroller – 1 avvik)
Styre konfigurasjonen (4 kontroller)
Styre servicenivå (4 kontroller)
Styre kapasitet (5 kontroller)
Styre tilgjengelighet (9 kontroller)
Styre brukertilgang (6 kontroller – 3 avvik)
Styre sikkerhet (32 kontroller – 5 avvik)
Styre prosjekter (4 kontroller – 1 avvik)
Styre leverandører (2 kontroller)

4.2 Hovedkonklusjon og sammendrag

Uttalelsen fra E&Y konkluderer positivt og Kommunerevisjonen mener at den underbygger vår oppfatning om at det er relativt lav risiko for vesentlig feilinformasjon på regnskaps- og regnskapspåstandsnivå for transaksjonsklasser, kontosaldoer og tilleggsopplysninger knyttet til drift av NLP i relevant periode i 2012.

Ernst & Young avdekket avvik i til sammen 14 kontroller. EVRY har gjennomgått avvikene, gitt kommentarer og beskrevet korrigerende tiltak inklusive tidsfrister.

4.3 Kommunikasjon

Ovennevnte er kommunisert til Utviklings- og kompetanseetaten i brev 18.02.2013.

[4] Evry ble til i 2012 etter en fusjon mellom EDB Business partner og ErgoGroup

[5] For eksempel overvåking og logging

5. Revisjon av nytt lønnssystem

5.1 Bakgrunn og formål

Agresso HR er i løpet av 2012 rullet ut i alle kommunens virksomheter samtidig med utfasingen av NLP. Lønnssystemet produserer vesentlige beløp for kommunen i form av lønn og godtgjørelser og håndterer vesentlige inntekter i form av sykelønnsrefusjoner fra NAV.

Kommunerevisjonen har gjennomgått deler av rutinene i og rundt HR systemet for å kartlegge vesentlige transaksjonsstrømmer og identifisere nøkkelkontroller som revisjonen basere revisjonen på for å utføre en effektiv revisjon. Ut fra dette skal vi fastsette et revisjonsopplegg som gir rimelig sikkerhet for at bokført lønn og refusjon ikke inneholder vesentlige feil eller mangler.

Vi har i tillegg undersøkt deler av datakonverteringen fra NLP til Agresso HR.

5.2 Hovedkonklusjon og sammendrag

Kartlegging av transaksjonsklasser og nøkkelkontroller
En transaksjonsklasse er en gruppe transaksjoner som er underlagt samme prosesser og kontroller (Nøyaktighet - fullstendighet - gyldighet). Nøkkelkontroller kjennetegnes ved at de kan, gitt at de etterleves og/eller fungerer hensiktsmessig, redusere eller eliminere hele eller vesentlige deler av kontrollrisikoen i en transaksjonsklasse. Regnskapsrevisjonen baserer mye av revisjonen på å teste etterlevelse av nøkkekontroller, som for eksempel at lønnsrapport for ledere blir kontrollert på riktig måte og i tilstrekkelig omfang.

Kartleggingen av HR-systemet har ikke avdekket vesentlige endringer i verken transaksjonsklasser eller nøkkelkontroller Sammenlignet med NLP. Dette innebærer at lønn i Agresso HR i all hovedsak vil bli revidert på samme måte som i NLP og at vi oppdaterer våre revisjonsprogram med terminologi og begreper fra Agresso HR.

Effektivisering av revisjonen
Agresso HR representerer teknologier som gir betydelige effektiviseringsmuligheter. Kommunerevisjonen har fått særskilt tilgang til funksjonalitet og data i Agresso HR, og jobber kontinuerlig med effektivisering av revisjonsarbeidet. Vi forventer ytterligere effektiviseringer i 2013 i takt med at vi opparbeider oss kompetanse på systemet.

IT-revisjoner
Kartleggingen av Agresso HR har bidratt til bedre prioritering av de IT-revisjonene som er obligatoriske i Agresso HR.

Konvertering av data fra NLP til HR
Både NLP og Agresso HR beregner lønn og refusjonskrav som en funksjon av registrerte data om personressurser og faste data. Systemene håndterer også akkumulerte data av betydning for innrapportering til sentrale myndigheter. Tidligere års revisjoner har ikke avdekket vesentlige feil eller mangler i datakvaliteten i NLP [6]. Kommunerevisjonen har derfor ment at dataene i NLP i det vesentligste har hatt tilstrekkelig kvalitet.

For å kunne bygge videre på datakvaliteten har vi evaluert konverteringen av lønnsdata fra NLP til Agresso HR. I gjennomgangen har vi blant annet vurdert om konverteringsmetodikken har vært hensiktsmessig, om virksomhetene har fulgt metodikken og om HR-prosjektet sentralt har fulgt opp virksomhetene på en god måte.

Undersøkelsene av virksomhetene har inngått som en del av ordinær lønnsrevisjon for 2012.

[6] Jf. kommunerevisjonens rapporter: 23/2005, 13/2009, 6/2010, 10/2010 og 4/2011

Kommunerevisjonen mener at metodikken i all hovedsak har vært hensiktsmessig for sitt formål og at gjennomføringen av konverteringen av data relatert til utbetaling av lønn synes å ha fungert som planlagt.

Gjennomføringen av konverteringen av fraværs-data synes ikke å ha fungert som forutsatt. En stund var det tvil om prosjektet ville komme i mål med konvertering av fraværsdata til årsavslutningen. Kommunerevisjonen mener at det på et for sent tidspunkt ble tatt tak i problemene med konverteringen av fraværsdataene. Revisjonen vil følge opp virksomhetenes håndtering av vesentlige avvik.

5.3 Kommunikasjon

Byrådsavdeling for finans er i brev av 21.02.2013 informert om revisjonens foreløpige konklusjoner om konverteringen. Vår avsluttende gjennomgang av konverteringene er en del av den ordinære regnskapsrevisjonen og pågår som en del av revisjon av årsregnskapet. Dersom det avdekkes vesentlige beløpsmessige feil eller mangler eller andre svakheter i intern kontrollene rundt konverteringen vil det bli rapportert som en del av regnskapsrevisjonen når denne er avsluttet.

6. Diverse revisjon av fellessystemer

6.1 Bakgrunn og formål

Agresso Business World (ABW) er Oslo kommunens felles økonomisystem og informasjonen i systemet danner grunnlag for kommunens regnskap. ABW er også et viktig verktøy i utførelsen av kommunerevisjonens revisjonshandlinger. Revisjonshandlingene hviler på en forutsetning om at datagrunnlaget i hovedbok, reskontro, og saldotabeller er fullstendig, gyldig og nøyaktig, samt at arbeidsdeling, fullmakter og tilganger er iht. kommunens retningslinjer. Revisjonshandlingene involverer blant annet bruk av den rapporterings-funksjonaliteten som ligger i systemets spørremaler og browser.

Etter innføringen av Agresso i 2002, avdekket vi store svakheter i tilgangsadministrasjonen. Tilgangsadministrasjonen er senere innskjerpet.

Etter innføringen av elektronisk fakturabehandling i 2006, avdekket vi store svakheter i tabeller, regelverk og loggføring som skulle ivareta arbeidsdeling i godkjenningsprosessen. Rutinene er senere endret og har i all hovedsak deretter fungert etter hensikten.

Vi har også avdekket avvik i regnskapsrapporter i forhold transaksjonsdatabasen, som skyldes svakheter i rutinene rundt endringer av regnskapsopplysninger og oppdatering tabeller. Rutinene har blitt endret ila 2011 og ser ut til å fungere som forutsatt (se pliktig regskapsrapportering).

Vår erfaring de senere årene peker på særskilt risiko ved innføring og endring av økonomisystemer.

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

6.2 Hovedkonklusjon og sammendrag

Arbeidsdeling i den elektroniske fakturabehandlingen
Etter innføringen av versjon 5.5 i juni 2011 har vi ikke funnet mangelfull arbeidsdeling på leverandørfakturaer. Det ser derfor ut til at innføringen av versjon 5.5 har medført at arbeidsdelingskontrollen fungerer som forutsatt.

Pliktig regnskapsrapportering
Den pliktige regnskapsrapporteringen skjer gjennom de predefinerte rapportmalene OKS 033, 034, 036 og 039. Disse er basert på saldotabeller som genereres ut fra ulike rapporteringsbegreper fra transaksjonstabeller i ABW og ser ut til å fungere som forutsatt.

Rapporteringsbegrepene er ikke en del av konteringsstrengen, og det vil som tidligere være viktig å ha kontroll på relasjonene (koblingene) mellom konteringsbegrepene og rapporteringsbegrepene.

For å fange opp eventuelle avvik mellom hovedbok og saldotabellene, er det etablert en rapport som sammenlikner aggregerte beløp i saldotabellene mot tilsvarende hovedboks-transaksjoner. Ved avvik blir Agresso brukerstøtte varslet på e-post. Denne rapporten ser ut til å fungere som forutsatt. I tillegg til de automatiske kontrollene skjer det en tilsvarende manuell kontroll i forbindelse med periodeavslutning.

Internkontrollgrunnlag
Virksomhetene bruker spesielt en spørring og en rapport i Agresso som grunnlag for intern kontroll av merverdiavgift. Både spørringen og rapporten ser ut til å fungere som forutsatt.

Tilganger som medfører både utbetalings- og bokføringsfullmakt

En sammenstilling av bokføringstilganger med utbetalingsfullmakter i DNB pr. virksomhet i 2012 avdekket en del forhold som vi har valgt å følge mot den enkelte virksomhet. Samlet resultat av dette vil ikke foreligge før revisjonen for 2012 er avsluttet.

6.3 Kommunikasjon

Denne IT revisjonen er en del av den ordinære regnskapsrevisjonen, og rapportering til revidert enhet skjer på samme måte som i regnskapsrevisjonen. Byrådsavdeling for finans er særskilt informert om innholdet i dette kapitlet. Dersom det avdekkes vesentlige svakheter i intern kontrollene ved de avsluttende revisjonshandlingene i regnskapsrevisjonen, vil det bli rapportert som en del av regnskaps-revisjonen når denne er avsluttet.

7. Revisjon av FAS og rutiner og kontroller knyttet til inntekter fra alarmabonnementer og unødige utrykninger

7.1 Bakgrunn og formål

Applikasjonen FAS benyttes ved 110-sentralen hos Brann- og redningsetaten. FAS genererer inntektsgrunnlag knyttet til alarmabonnementer og unødige utrykninger. Inntektene for disse utgjorde i 2012 ca. 24 mill. kr for alarm-abonnementer og ca. 10,5 mill. kr for unødige utrykninger.

Revisjonens formål er å sikre fullstendighet for inntektene for alarmabonnement og unødige utrykninger. Herunder gjennomgang og vurdering av IT-miljøet i og rundt applikasjonen FAS, grensesnittet mellom FAS og Agresso, samt fakturering og bokføring i Agresso.

7.2 Hovedkonklusjon og sammendrag

Vi har observert svakheter i alle de gjennom-gåtte IT-prosessene endringshåndtering, tilgangskontroller, IT-organisering, risiko-styring og driftskontinuitet. I hovedsak er svakhetene knyttet til manglende skriftlige rutinebeskrivelser og manglende prosedyrer. Etaten opplyste at det pågikk et arbeid med et informasjonssikkerhetsdokument som skulle rapporteres til byrådsavdelingen i løpet av november 2012.

For grensesnittet mellom FAS og Agresso og kontroller i og rundt Agresso har vi observert svakheter på flere områder, i hovedsak knyttet til manglende rutinebeskrivelser, manglende dokumentasjon av gjennomførte kontroller og manglende arbeidsdeling i inntektsprosessene.

Testing av et utvalg transaksjoner i regnskapet (utgående fakturaer og kreditnotaer) avdekket også enkelte feil og mangler knyttet til de forskjellige inntektsprosessene for alarm-abonnementer og unødige utrykninger.

Samlet sett medfører svakhetene en risiko for at regnskapsførte inntekter ikke blir korrekte og fullstendige.

7.3 Kommunikasjon

Revisjonen ble rapportert til etaten høsten 2012. Brann- og redningsetaten har i sitt svar til Kommunerevisjonen sagt at de tar de kommenterte forholdene til etterretning og vil foreta en gjennomgang av aktuelle rutiner. Etaten vil komme tilbake med nærmere svar når en slik gjennomgang er utført.

8. Lokal og sentral tilgangsadministrasjon i SATS barnehage

8.1 Bakgrunn og formål

SATS barnehage benyttes av alle bydeler i forbindelse med registrering av opplysninger relatert til barn i barnehage og beregning av månedlig oppholdsbetaling for disse. Byrådsavdeling for kultur og næring er systemeier, Helseetaten er systemansvarlig og bydelene er brukere av systemet. Oslo kommunes inntekter generert gjennom oppholdsbetaling ved barnehagene var omtrent 441 millioner i 2011.

Revisjonens formål er å innhente rimelig sikkerhet for at regnskapene ikke inneholder vesentlige feil i inntektene som følge av svakheter i brukeradministrasjonen i SATS barnehage.

8.2 Hovedkonklusjon og sammendrag

Brukeradministrasjon
I henhold til Rutinehåndboken er den enkelte bydel ansvarlig for å håndtere bruker-administrasjonen i SATS barnehage. Tilgang til SATS barnehage gis ved at bemyndiget person ved bydelen godkjenner den nye brukeren på standard autorisasjonsskjema. Det er ikke lagt føringer for hvordan disse skjemaene skal oppbevares eller hvor lenge de skal oppbevares i bydelene. Det er ikke noe krav om eller felles rutine for årlig gjennomgang av bruker-tilgangene.

Ved tildeling av tilganger til SATS barnehage skal tilgangsnivået vurderes ut fra hvilket behov den enkelte bruker har. Dersom en ny bruker opprettes uten tilgangsnivå og uten tilgangsgruppe, får man automatisk full tilgang til systemet.

Brukerautorisasjon og gjennomgang av brukere ved bydelene

Grunnlag for vår kontroll var en oversikt fra Helseetaten over gjeldende tilganger til SATS barnehage. Oversikten viste 149 tilganger per 07.06.2012. Tilganger i henhold til oversikten ble sendt de respektive bydelene for gjennomgang og tilbakemelding ble deretter gitt til kommunerevisjonen. Resultatet av undersøkelsen viste at 49 av de registrerte brukerne ikke lenger hadde behov for tilgang til SATS barnehage, enten fordi de hadde sluttet i bydelen eller hadde fått andre arbeidsoppgaver. Det var kun to bydeler hvor aktive tilganger var i samsvar med oversikten fra Helseetaten, for seks av bydelene viste tilbakemeldingen at antall tilganger burde vært redusert med fem eller flere brukere. Ved tre av bydelene var det opprett to tilganger til samme bruker slik at brukere kunne utføre forskjellige funksjoner samtidig, den ene bydelen har nå slettet den ene tilgangen for sin bruker mens de to andre bydelene opprettholdt begge til-gangene. Brukere legges inn i systemet uten fullt navn, slik at kun brukeridenten vises på tilgangsoversiktene

8.3 Kommunikasjon

Oppsummering av revisjonen ble sendt per brev til Byrådsavdeling for kultur og næring med kopi til bydelene. Byrådsavdeling for kultur og næring skriver i sitt svarbrev til kommune-revisjonen at det er sendt et brev til alle bydelene hvor byrådsavdelingen ber bydelene følge de anbefalinger Kommunerevisjonen gir og sørge for at mangler ved tilgangskontrollen korrigeres.

Byrådsavdelingen ber også bydelene sørge for at oppfølging av gjeldende rutiner er innarbeidet i bydelen slik at tilsvarende feil ikke oppstår.

9. Revisjon av Xpand og husleieinntekter

9.1 Bakgrunn og formål

Xpand er Omsorgsbyggs system for forvaltning, drift og vedlikehold av eiendommer, herunder beregning av husleieinntekter. Systemet ble satt i drift i 2010. Det samlede bygningsarealet er på ca. 930 000 m2 og er fordelt på over 1 100 bygg. Husleieinntektene som gikk gjennom Xpand var for 2011 i overkant av 1 milliard kroner, 970 millioner i intern husleie og 46 millioner i husleie til eksterne leietakere.

Revisjonens formål er å innhente rimelig sikkerhet for fullstendighet og nøyaktighet i husleieinntektene.

9.2 Hovedkonklusjon og sammendrag

Tilgangskontroller og endringshåndtering
Vi har observert svakheter i IT-prosessene endringshåndtering og tilgangskontroller, i hovedsak er dette knyttet til manglende skriftlige rutinebeskrivelser og prosedyrer. Foretaket har opplyst om at de jobber med å utarbeide skriftlige rutinebeskrivelser på begge områder. Det er manglende oppfølging av logger i Xpand, noe som øker risikoen for at uvanlige og uautoriserte hendelser ikke blir oppdaget.

Bruk og nytte av Xpand
Pr. i dag ligger prosjektkalkyle og husleie-kalkulator i Excel mens fakturering og bokføring håndteres i Agresso. Bruken av Xpand til å formidle økonomisk informasjon innebærer således et ekstra ledd i faktureringen, og derfor også en tilleggsrisiko for at bevisste og ubevisste feil kan oppstå.

Fakturering
Ved vår test av utvalgte eiendommer mot det som er fakturert, har vi i vår stikkprøvekontroll avdekket to tilfeller av overfakturering. Foretaket har opplyst at dette vil bli korrigert.

9.3 Kommunikasjon

Oppsummering av revisjonen ble sendt per brev til foretaket med kopi til Byrådsavdeling for kultur og næring 03.01.2013. Foretaket skriver i sitt svarbrev til Kommunerevisjonen at de tar oppsummeringen i brevet til etterretning og vil sørge for at områdene som mangler skriftlige rutiner blir fulgt opp og lagt inn i foretakets KS-system. Det vil også bli gjennomført interne kontroller for å sikre at alle nye anlegg blir fakturert.

10. Revisjon av inntekter fra Ungbo via Concorde

10.1 Bakgrunn og formål

Concorde benyttes av Ungbo i forbindelse med forvaltning av boliger, herunder husleieinntekter. Velferdsetaten er systemeier fra og med 2012. Systemet anses som virksomhetskritisk, inntektene utgjorde ca. kr 15 mill. i 2011. Systemet ble innført i Oslo kommune i 1988 og etter våre opplysninger ble vedlikeholdsavtalen med leverandøren sagt opp i 2004 og systemet har derfor ikke vært gjenstand for vedlikehold etter dette. Leverandøren har ikke lenger tilbud om brukerstøtte/utvikling av Concorde.

Revisjonens formål er å innhente rimelig sikkerhet for at regnskapene ikke inneholder vesentlige feil i inntektene ved virksomheten som følge av svakheter ved driften i IT-systemet Concorde.

10.2 Hovedkonklusjon og sammendrag

Det er ikke utarbeidet særskilt beredskapsplan eller definert tilgjengelighetskrav for Concorde. Oslo kommunes driftsleverandør Evry drifter Concorde og foretar sikkerhetskopiering av Concorde på lik linje med andre systemer på vegne av Oslo kommune slik at det ved midlertidig driftsavbrudd er mulig å tilbakeføre data. Hvis det skulle oppstå en situasjon hvor systemet ikke lenger fungerer vil det imidlertid ikke være mulig å legge tilbake en sikkerhetskopi fordi Concorde da ikke lenger vil være tilgjengelig.

Concorde logger alle hendelser i systemet, men det er ikke etablert rutiner for hvilke hendelser som skal kontrolleres. Det foretas ingen kontroll av loggene. Det har ikke vært foretatt sletting av data i loggen i perioden siden oppstarten av Concorde i 1988.

10.3 Kommunikasjon

Oppsummering av revisjonen ble sendt per brev til Velferdsetaten med kopi til Byrådsavdeling for eldre og sosiale tjenester. Velferdsetaten skriver i sitt svarbrev til Kommunerevisjonen at virksomheten er enig med Kommunerevisjonen i at det er behov for nye IT-løsninger for Ungbo som sikrer husleieinntekter og journaler knyttet til den enkelte beboer. Virksomheten har iverksatt en gjennomgang av Ungbo som også vil omfatte en vurdering av forvaltnings- og kvalitetssystem for tjenesten. Gjennomgangen er forventet avsluttet i mars 2013. Virksomheten vil også se på ordninger som på kort sikt vil bedre situasjonen. Det er også opprettet en hurtigarbeidende arbeidsgruppe som skal se på løsninger på kort sikt for å ivareta nødvendig driftssikkerhet og ha ansvar for å gjennomføre kontroll/gjennomgang av logger.

11. Revisjon av Picasso og gjennomgang av inntekter ved Øvingshotellet

11.1 Bakgrunn og formål

Picasso ble anskaffet av Kulturetaten og tatt i bruk av Øvingshotellet i 2011. Picasso benyttes til booking av rom og økonomioppfølging. De fleste betaler kontant etter bruk, mens noen blir fakturert. I 2011 var det 3,2 mill. i inntekter som ble generert i Picasso. Systemet er forholdvis nytt, og det er derfor foretatt en vurdering/ revisjon av systemet og rutinene.

Revisjonens formål er å innhente rimelig sikkerhet for at regnskapene ikke inneholder vesentlige feil som følge av forvaltningen og bruken av bookingsystemet Picasso.

11.2 Hovedkonklusjon og sammendrag

Forvaltning av Picasso
Øvingshotellet er kjent med at systemets funksjonalitet ikke dekker virksomhetens behov. Virksomheten har imidlertid ikke gjennomført en risikovurdering av systemet. Det er derfor usikkert om de etablerte kontrollene i og rundt systemet er hensiktsmessige. Denne usikkerheten og den mangelfulle funksjonaliteten gjør at risikoen knyttet til elektronisk behandling av inntekter ikke er tilstrekkelig håndtert.

Brukerdokumentasjon og opplæring
Brukerdokumentasjonen og opplæringen tilrettelegger for hensiktsmessig bruk av systemet.

System- og brukeradministrasjon
Picasso tillater svake passord, og Øvingshotellet har ikke definert krav til passordkompleksitet og passordskifte. Systemet har loggfunksjonalitet, men Øvingshotellet har ikke etablert rutiner for gjennomgang av logger. Uautoriserte endringer i dataene blir derfor ikke oppdaget.

Kundebehandlere har ikke tilgang til systemparametere og tilgangs-administrasjon. Men det er ikke etablert arbeidsdeling mellom de som foretar bookinger, og de som tar imot betalinger eller fakturerer. To brukere hadde tilgang til systemet selv om de ikke hadde behov for den. Vi har også oppdaget at to personer hadde tilganger som medfører svak arbeidsdeling.

Gjennomgang av inntektene
Timeantall registreres manuelt i systemet, og rompris velges fra en rullegardinmeny. Begge deler kan endres manuelt underveis. Dette øker risikoen for at bookinger ikke faktureres eller faktureres med lavere pris enn det skal. Det er ikke etablert uavhengig kontroll av timeantall og pris på vanlige kunder.
Manuell inntasting av beløp til betaling i både systemet og bankterminalen øker risikoen for feil, men uoverensstemmelser vil bli oppdaget ved dagsavstemming. Uavhengig kontroll av dagsavstemminger reduserer risikoen for feil.
Øvingshotellet kontrollerer ikke om dags-/ ukesrapportene blir fullstendig og korrekt bokført i Agresso.
Det er ikke etablert en uavhengig kontroll av kunderegistrering i Agresso eller av faktureringen som foretas med grunnlag i Picasso.
Øvingshotellet bør etablere rutine for å kontrollere om de overførte fakturagrunnlagene faktisk blir fakturert og inntektsført f.eks. ved at sum oversendte fakturaer fra Picasso blir avstemt mot sum inntektsført i Agresso.

11.3 Kommunikasjon

Oppsummering av revisjonen ble sendt per brev til Kulturetaten med kopi til Byrådsavdeling for kultur og næring 24.10.2012. Vi har foreløpig ikke mottatt noe svar på vårt brev fra etaten.

12. Generelle it kontroller i PAX, oppfølging av fjorårets revisjon

12.1 Bakgrunn og formål

PAX er Kemnerkontorets system for fakturering, regnskapsføring og innkreving av gebyrer for Trafikketaten. Parkeringsgebyr (inkl. piggdekk- og miljøgebyr) og forhøyelser ved forsinket betaling utgjorde ca. 140 mill. i 2012.

På bakgrunn av Kommunerevisjonens rapport om IT- systemet PAX utstedt i 2011, er det foretatt en oppfølging av generelle IT- kontroller hos Kemnerkontoret våren 2012.

12.2 Konklusjon og sammendrag

Endringshåndtering
2011:Kemnerkontoret har en prosedyre for håndtering av endringsønsker for PAX, men endringshåndteringen i etaten er ikke formalisert.
2012: Kommunerevisjonen har fått utlevert en rutinebeskrivelse for endringsstyring i PAX. Når det gjelder testing av endringer så ser vi at IT-avdelingens eventuelle kompabilitetstesting ikke er omtalt i rutinen.

Brukeradministrasjon
2011:Kemnerkontoret mangler skriftlige rutiner for brukeradministrasjon. De etablerte rutinene etterleves ikke alltid og dette blir ikke fulgt opp. Som en konsekvens av dette, mangler enkelte eksisterende tilganger til PAX skriftlig autorisasjon – noe som vanskeliggjør gjennomgang av tilganger.
2012: Kommunerevisjonen har fått utlevert en skriftlig rutine for opprettelse av brukertilgang hos Kemnerkontoret. Rutinen for oppfølging av brukere i PAX er mindre presis.

Tilgangskontroller
2011: Tilgangsrapportene gir mangelfull og ikke-korrekt oversikt over brukerne, rollene og tilgangsrettighetene. Det lar seg ikke bekrefte at gitte tilganger stemmer med autorisasjoner. Det er etablert arbeidsdeling mellom bestilling og implementering av tilganger, men kontrollfunksjon mangler – rollene og brukerkontoene gjennomgås ikke regelmessig.
2012: Kemnerkontoret har avdekket tilfredsstillende tilgangsoversikter i PAX. Man venter også på neste versjon av PAX der tilgangsadministrasjonen/roller er forbedret. Det er etablert en rutine for regelmessig gjennomgang av brukere og tilknyttede roller (jf. formell rutine for oppfølging av brukere i PAX), men ikke innholdet i rollene.

Tilgang til administratorrollen i PAX
2011: Kommunerevisjonen anser at antall PAX-brukere med administratorrollen var unødvendig stort på revisjonstidspunktet. Tilgangen er gitt til 14 brukere til sammen.
2012: Administratorrollen er gitt 11 brukere, b.la til regnskapsansvarlig.

Passordsikkerhet
2011: Passordreglene tillater svake passord, i tillegg til at manglende passordvalidering gjør det mulig for brukere å lage enda svakere passord.
2012: Sikkerhetshåndboken stiller krav til passordsikkerhet. Kravet til passordkompleksitet synes ikke å være tilfredsstillende, og kravet til passordbytte er ikke presist.

Loggfunksjonalitet
2011: Låsing av journaler kompenserer delvis for mangelfull logging og loggjennomgang, men uvanlige og uautoriserte hendelser knyttet til bruker- og systemadministrasjon i PAX vil ikke bli oppdaget.
2012: Kemnerkontoret er ikke kjent med loggoppbygningen og har derfor ikke definert kriterier og rutiner for oppfølging av logger.

12.3 Kommunikasjon

Oppsummering av oppfølgingen fra 2011 ble sendt pr. brev til Kemnerkontoret med kopi til Byrådsavdeling for finans 28.08.2012. Virksomheten har svart på brevet med tiltak på hver enkelt av våre observasjoner.

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 - 02.13