Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C

Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

Københavns Kommune
Koncernservice
Att.: Direktør Kasper Schmidt
Borups Alle 177
2400 København NV

Revisionsrapport – Revision af generelle it-kontroller 2014

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2014 har vi foretaget revision af generelle it-kontroller.

Rapporteringen er opbygget på følgende måde:

1. Formål og omfang mv.
2. Ledelsesresume og konklusioner
3. Observationer, risikovurderinger og anbefalinger
4. Formidling af risiko og væsentlighed

1. Formål, omfang mv.

1.1. Revisionens formål

Revision af de generelle it-kontroller er en del af den lovpligtige revision og indgår i grundlaget for vores påtegning af Københavns Kommunes årsregnskab. De generelle it-kontroller er de kontroller, som er etableret i og omkring virksomhedens væsentlige it-platforme med henblik på at opnå en velkontrolleret og sikker it-anvendelse, og dermed også understøtte de it-baserede forretningsprocesser, som har betydning for Københavns Kommunes regnskabsaflæggelse.

Revisionens formål er at undersøge, om de generelle it-kontroller er udformet og implementeret på en hensigtsmæssig måde vedrørende KØR og Navision (i TMF), samt hvorvidt kontrollerne har fungeret i hele revisionsperioden vedrørende KØR.

Det bedste værn mod uregelmæssigheder er hensigtsmæssige forretningsgange og gode interne kontroller, hvorfor vores revision i vidt omfang har baseret sig på efterprøvelse af forretningsgange og interne kontroller, men ikke undersøgelser specielt med henblik på opdagelse af uregelmæssigheder.

Det påhviler ledelsen at tilrettelægge kontrolsystemer og forretningsgange, der er betryggende efter kommunens forhold, og det påhviler revisor at gennemgå disse forretningsgange og interne kontroller som et led i revisionen af årsregnskabet.

1.2. Revisionens omfang og afgrænsning

Revisionen er baseret på en forventning om, at der er tilrettelagt et velfungerende internt kontrolsystem og en pålidelig bogføring. Dette indebærer, at det overordnede kontrolmiljø og de organisatoriske rammer understøtter et velfungerende ledelses- og kontrolsystem, og at der på de enkelte aktivitetsområder er beskrevet og implementeret interne kontroller, som reducerer risikoen for væsentlige fejl til et acceptabelt niveau.

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for væsentlig fejl.

Revisionen har omfattet en vurdering af kontrollerne inden for nedennævnte områder. Revisionen er tilrettelagt således, at ikke alle områder gennemgås lige detaljeret hvert år, dog således at væsentlige kontrolsvagheder altid bliver fulgt op ved efterfølgendes års revision.

- It-sikkerhedsstyring: Primært tilstedeværelsen af it-risikoanalyse, it-sikkerhedspolitik og it-beredskabsplan
- It-sikkerhedsadministration: Særligt fokus på processer for oprettelse, nedlæggelse og periodisk review af brugeradgange samt politik for logning
- Logisk sikkerhed: Kort opfølgning på udvalgte, implementerede sikkerhedsparametre på udvalgte platforme
- Change management: Processer for vedligeholdelse af KØR og TMF

Revisionen af de generelle it-kontroller har ikke omfattet en vurdering af kontrol- og sikkerhedsniveauet i de enkelte brugersystemer, herunder automatiske kontroller i de administrative processer og logiske adgangsrettigheder til udførelse af forretningsaktiviteter i brugersystemerne.

Københavns Kommune har aftale med KMD omkring drift af væsentlige systemer og tilhørende platforme.

Der modtages årligt en revisionserklæring for de generelle it-kontroller omfattende de fælleskommunale systemer, som driftes hos KMD. Øvrige Københavns Kommune specifikke systemer, herunder

KØR, Udbudsportalen og Vagtplan, som ikke er omfattet af den generelle erklæring fra KMD, og forventes gennemgået af Deloitte hos KMD i foråret 2015.

Vi skal for god ordens skyld gøre opmærksom på, at revisionen først kan anses for afsluttet, når vi har underskrevet erklæringen på årsregnskabet.

1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2014 og ved interview af relevant personale hos Københavns Kommune samt ved observation, gennemgang af udleveret materiale samt gennemgang af den tekniske sikkerhedsopsætning på udvalgt platform.

2. Ledelsesresume og konklusion

Revisionen af de generelle it-kontoroller har givet anledning til følgende væsentlige forhold som bør forbedres:

- Der er ikke foretaget en gennemgang af tildelte rettigheder til brugere på KØR (observation 3.2)
- Udviklere har "ikke overvåget" adgang til TMF-Navision produktionsmiljø (observation 3.6)

Revisionen har herudover ikke givet anledning til bemærkninger.

3. Observationer, risikovurdering og anbefaling

Oversigt over observationer

Organisationsområde i KK	Koncernservice (KS)	Revisionsområde/ emne	Generelle it-kontroller

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed
3.1 It-sikkerhedsledelse og it-risikoanalyse	Vi har fået oplyst, at KK i samarbejde med PwC, har foretaget en modenhedsanalyse som har resulteret i en risikostyringsmodel, der beskriver de aktiviteter, som skal udføres for at skabe et samlet risikobillede. Risikostyringsmodellen er forelagt til bestyrelses-godkendelse. KK forventer, at risikoanalyser for de enkelte forvaltninger udarbejdes i løbet af 2015.	En manglende eller utilstrækkelig it-risikoanalyse medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici som vurderes som relevante.	Vi skal anbefale, at gennemførelsen af it-risikovurderinger følger kravene i IT-sikkerhedsregulativet, og at de gennemføres snarest muligt.	
3.2 Brugerrettigheder – periodiske ervurdering (AD-KØR)	Vi har konstateret, at der er etableret kørsler og rapporter, som kan benyttes til periodisk revurdering af tildelte rettigheder til KØR og AD'et. Vi har dog fået oplyst, at disse kørsler ikke er afviklet på nuværende tidspunkt, men at dette vil blive gennemført i løbet af 2015. Det skal bemærkes, at samme handlingsplan blev fastlagt sidste år, uden det dog har fundet sted.	Manglende eller utilstrækkelig periodisk revurdering af tildelte rettigheder til brugere medfører risiko for, at brugeres rettigheder bliver utidssvarende og ikke afspejler deres arbejdsmæssige betingede behov.	Vi skal anbefale, at der med udgangspunkt i de etablerede kørsler periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere for relevante systemer og platforme. Ansvaret herfor ligger i forvaltningerne for egne brugere.	

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed
3.3 It-sikkerhedslogning (AD, KØR, TMF)	Vi har fået oplyst, at logningskrav ikke er formelt defineret for de tre områder, som er inkluderet i denne revision, dvs. Windows netværket, KØR og Navision TMF applikationerne, herunder også de underliggende databaser. Vi har dog konstateret, at der er etableret it-sikkerhedslogning på den reviderede Windows platform "Navision TMF Microsoft SQL" server. Endvidere har vi fået oplyst, at der ikke er etableret periodisk review af de logs, som på nuværende tidspunkt er etableret. Vi har fået oplyst for hhv. Windows netværk, KØR og Navision TMF, at notater vil blive udarbejdet indeholdende krav til it-sikkerhedslogning, herunder også beskrivelse af, hvorledes der skal følges op på logs.	Manglende eller utilstrækkelig sikkerhedsmæssig logning medfører risiko for, at forsøg på uautoriserede handlinger ikke opdages og imødegås i tilstrækkeligt omfang.	Vi anbefaler, at der etableres en procedure for håndtering af logs, herunder en beskrivelse af logkrav, samt hvorledes der skal følges op på logs. Endvidere anbefaler vi, at systemejer formelt godkender denne logprocedure samt sikrer, at logproceduren er implementeret som vedtaget.	
3.4 Ændringskontrol – fall-back (KØR)	Vi har fået oplyst, at der i forbindelse med implementering af ændringer til produktionsmiljøet uformelt tages stilling til, hvorledes fallback kan gennemføres, såfremt ændringerne mod forventning skulle medføre problemer i produktionsmiljøet. Overvejelserne dokumenteres dog ikke, ligesom det ikke fremgår, hvorvidt eventuelle forudsætninger for fallback kontrolleres, f.eks. at der er taget en sikkerhedskopi forinden implementering af ændringerne. Det er dog oplyst, at det forventes, at KMD kan foretage en eventuel reetablering til stadiet før implementeringen, såfremt ændringen medfører fejl.	Manglende eller utilstrækkelig planlægning af fallback medfører risiko for unødige komplikationer i forbindelse med, at fejlbehæftede ændringer implementeret i produktionsmiljøet, forsøges fjernet igen.	Vi skal anbefale, at overvejelserne omkring fallback dokumenteres og godkendes i forbindelse med implementeringen af ændringer til produktionsmiljøet, og at eventuel kontrol af forudsætningerne for fallback tillige dokumenteres.	
3.5 Bruger-rettigheder og funktionsadskillelse i TMF	Vi har fået oplyst, at der ikke er foretaget formelle vurderinger af, hvorvidt der er etableret tilstrækkelig systemmæssig funktionsadskillelse i Navision.	Manglende eller svage procedurer vedrørende administration og vedligeholdelse af adgange til systemer medfører øget risiko for tildelte adgangsrettigheder overstiger brugerens arbejdsmæssige betingede behov eller ikke understøtter virksomhedens organisatoriske opdeling af arbejdsopgaver.	Vi anbefaler, at der foretages en formel vurdering af funktionsadskillelsen på applikationsniveau, således at der på baggrund af en konkret risikovurdering, udarbejdes en oversigt over roller / adgangsrettigheder, der ud fra ønsket om opretholdelse af en organisatorisk funktionsadskillelse, ikke bør tildeles til samme bruger.	

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed
3.6 Ændringskontrol – adgangskontrol til miljøer (TMF)	Vi har fået oplyst, at to personer fra Navision gruppen har et separat windows-login til Navision systemet, som benyttes til at idriftsætte ændringer. Dette login medfører endvidere, at de to personer har mulighed for at introducere ændringer direkte i produktionssystemet, på trods af deres rolle som interne udviklere i kommunen. Vi har endvidere fået oplyst, at brugen af disse konti ikke overvåges ved fx loggennemgang. Det er dog også oplyst, at Windows AD logger brugen af disse konti, således at logovervågning er mulig, f.eks. ved sammenholdelse af Windows logs med idriftsættelses-loggen. Afslutningsvis har vi fået oplyst, at TMF gruppen vil etablere en kontrol, der sikrer opfølgning på, at idriftsatte ændringer er i overensstemmelse med loggen i Navision.	Manglende eller utilstrækkelig kontrol med udvikleres adgange til produktionsmiljøer medfører risiko for, at fejl eller ændringer utilsigtet introduceres i produktionsmiljøet.	Vi skal anbefale, at "Application Builder" licensrettigheden fjernes fra den applikationslicens, der anvendes på produktionssystemet. Derved vil der ske en reduktion i, hvad der kan ændres direkte i produktionsmiljøet. Vi er bekendt med, at der i dag sker registrering af, hvem der har udviklet, eller hvem som står som ansvarlig for en given ændring, samt hvem der har indlæst ændringen i produktionsmiljøet. Vi anbefaler derfor, at der etableres en kontrol, der sikrer imod personsammenfald mellem udvikler / opgaveansvarlig og den, der idriftsætter, samt at denne kontrol dokumenteres. Endvidere anbefaler vi, at Københavns Kommune gennemfører en vurdering af, hvilke logs som kan være relevante at gennemgå periodisk (herunder fx logs fra Windows Domænet, logs fra SQL databasen, samt logs fra Navision). Disse logs kan endvidere benyttes til en kontrol af, at alle logons med en bruger, som har rettigheder til at ændre kode, kun er sket, når der har foreligget en godkendt ændringsanmodning.	

4. Formidling af risiko og væsentlighed mv.

Vi har vurderet graden af risiko og væsentlighed for de enkelte observationer. Risiko og væsentlighed er målrettet den reviderede decentrale enhed, hvor fejl kun ekstraordinært vil kunne give en fejl i det samlede regnskab. I tilknytning til den givne observation har vi påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med 🔴

- Prioritet 1 markeringer anvendes for risici, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en revisionsbemærkning
- En risiko anses for kritisk, såfremt der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt og/eller har en betydelig udbredelse
- Observationen medtages i delberetninger og beretninger til Borgerrepræsentationen

Prioritet 2 – markeres med 🟡

- Prioritet 2 markeringer anvendes for risici, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre revisionsbemærkninger i årsberetningen
- En risiko anses for væsentlig, såfremt der er en middel grad af sandsynlighed for at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse
- Observationen medtages ikke i delberetninger og beretninger

Prioritet 3 – markeres med 🟢

- Anvendes for risici, der anses for mindre væsentlige, og som derfor kun rapporteres til ledelsen som opmærksomhedspunkter
- En risiko anses for mindre væsentlig, såfremt der er en lille grad af sandsynlighed for at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse

5. Afslutning

Nærværende rapport har i udkast været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

Yderligere spørgsmål eller kommentarer til rapporten kan rettes til Lynge Skovgaard på telefon 3094 4828 eller Mikkel Jon Larssen på telefon 3070 4334.

København, den 5. marts 2015

Deloitte
Statsautoriseret Revisionspartnerselskab

Lynge Skovgaard
statsautoriseret revisor

Mikkel Jon Larssen
partner, CISA

cc. Jakob Joensen
Intern Revision