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.: Jens Ingemann
Borups Alle 177
2400 København NV

Revisionsrapport – Revision af generelle it-kontroller 2016

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2016 har vi foretaget revision af de generelle it-kontroller, som understøtter kommunens regnskabsaflæggelse.

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 vel-kontrolleret 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 i regnskabsaflæggelsen.

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 december måned 2016. Denne gennemgang resulterer i en specifik erklæring for de nævnte systemer, som foreligger i endelig ultimo januar 2017.

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 2016 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

På baggrund af vores revision af de generelle it-kontroller, som vi har vurderet relevante for at understøtte revisionen af årsrapporten for Københavns Kommune, har vi ikke identificeret væsentlige svagheder.

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. **Status 2016** Vi har konstateret, at it-risikoanalysen er gennemført for it-infrastruktur. Vi har fået oplyst, at risikovurderinger forventes udarbejdet for alle kritiske systemer i 2017 i forbindelse med at den centrale It-sikkerhedsfunktion overtager ansvaret for risikostyrings-processen i forvaltningerne med virkning fra januar 2017.	En manglende eller utilstrækkelig it-risikoanalyse medfører risiko for, at det etablerede it-sikkerheds-niveau 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. **Ledelsens kommentarer:** Koncern IT / It-sikkerhedsfunktionen har udformet ny risikostyringsproces, udarbejdet relevante værktøjer og etableret årshjul samt model for risikovurderinger i Københavns Kommune. Processer omfatter også risikovurdering i forbindelse med ad hoc vurderinger i forbindelse med it-anskaffelser mv. Proces iværksættes ved KIT's overtagelse af risikostyringsopgaven i nyt centralt IT-risikoanalyseteam pr. 1. Januar 2017. Der iværksættes sideløbende i samarbejde med forvaltningerne en proces med henblik på løbende forbedring og optimering af proces og tilhørende værktøjer.	
3.2 Brugerrettigheder – Periodisk revurdering (KSP-CICS)	Vi har fået oplyst, at gennemgang af tildelte almindelige brugerrettigheder i KSP-CICS ikke er foretaget. Det oplyses endvidere, at området vil være blandt indsatsområderne for 2016. Kommunen har i januar 2016 afsluttet en revurdering af tildelte adgange til brugeradministration i KSP-CICS, som har givet anledning til enkelte justeringer og opfølgningspunkter. **Status 2016** Vi kan konstatere at der i 2016 er gennemført review af kritiske rettigheder i KSP-CICS. Punktet lukkes..			

3.3 It-sikkerhedslogning	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. **Status 2016** Vi har konstateret, at logningskrav er overordnet defineret i de udvidede sikkerhedsregler men fortsat ikke er konkret udmøntet for relevante systemer og platforme. Det er endvidere oplyst, at logmanagement værktøjet LogPoint er implementeret, og der pågår en proces for at etablere overvågning af logs fra relevante systemer, der udvælges ud fra en risikovurdering. Kommunen forventer, at projektet vedrørende vurdering af logs samt procedure for gennemgang af disse for kommunens kritiske systemer vil blive gennemført i løbet af 2017.	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. Ydermere anbefaler vi, at periodisk gennemgang af relevante logs dokumenteres. **Ledelsens kommentarer:** Systemejer for AD vil i 2017 udarbejde en formel beskrivelse af de allerede eksisterende GPO`er (logningspunkter) i AD. Ydermere vil systemejer udarbejde proces beskrivelse for kontrol af logs. Spørgsmålet om Logning og tilhørende kontroller vil i øvrigt indgå som en naturlig del af risikovurderingsteamets arbejde jf. pkt. 3.1.	

3.4 Ændringskontrol – fallback (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. **Status 2016** Vi har konstateret, at der for releases er taget stilling til fallback. Punktet lukkes	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. **Status 2016** Vi kan konstatere at der ved oprettelse bliver taget stilling til roller og rettigheder. Derudover er der implementeret en kompenserende kontrol der overvåger medarbejdere med udvidede rettigheder, herunder hvorvidt disse medarbejdere laver bogføring. Punktet lukkes	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
3.7 Windows AD (TMF)-No Password Expiration	Vi har konstateret, at 10 aktive personlige brugerprofiler er undtaget fra den generelle politik for periodisk ændring af passwords. Vi har efterfølgende fået oplyst, at samtlige brugere nu er underlagt KK's generelle skift af passwords hver 90. dage. Derudover har vi konstateret, at profilen KK$ er undtaget fra brug af password. **Status 2016** Vi kan konstatere at der er brugere med no password expiration, samt at der ikke kan redegøres for hvorfor denne indstilling er anvendt. Observation vedr. KK$ lukkes, da dette er et Forest Object, og ikke en reel bruger.	Manglende krav om periodisk skift af password for brugerprofiler medfører øget risiko for, at sådanne passwords med tiden bliver kendte af andre, hvormed sikkerheden på systemet kan blive kompromitteret.	Vi anbefaler, at alle personlige brugerprofiler er forpligtet til at følge de overordnede krav om periodiske ændring af password. Endvidere anbefaler vi, at alle personlige brugerprofiler underlægges krav om brug af password. For profiler, hvor det er besluttet, at disse ikke skal anvende password, anbefaler vi at der foreligger dokumentation samt godkendelse herfor. **Ledelsens kommentarer:** Koncern IT vil iværksætte en undersøgelse af årsag til eksistens af brugerkonti, hvor egenskaben "Password never expieres" er sat. Der vil herefter blive iværksat en handlingsplan, der vil indeholde en proces for ændring af de brugerkonti, hvor egenskaben ikke skal være gældende samt fastlægge proces for dokumentation og kontrol.	
3.8 Windows AD (TMF) -Administrators	Vi har konstateret, at 31 personlige brugerprofiler er tildelt Administratorrettigheder og 77 brugerprofiler er medlemmer af brugergrupper med administratorrettigheder. Listen er verificeret af den ansvarlige hos KK. Vi har efterfølgende fået oplyst, at der er igangsat en undersøgelse af 9 brugere, som er tildelt udvidede rettigheder i kraft af deres administrator profil eller medlemskab af brugergrupper og som ikke alle længere har tilknytning til KS. **Status 2016** Vi kan konstatere at antallet af administratorer er nedbragt. Punktet lukkes	Tildeling af administrative privilegier til for mange brugerprofiler medfører risiko for, at sikkerheden ikke kan opretholdes på systemet.	Vi anbefaler, at antallet af brugerprofiler med administrative privilegier revurderes og nedbringes såfremt muligt. Endvidere anbefaler vi, at der etableres procedure for periodiske gennemgang af tildelte udvidede rettigheder til brugere.	

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

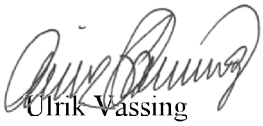
5. Afslutning

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 Ulrik Vassing på telefon 2220 2253 eller Lars Holm Sørensen på telefon 4079 4200.

København, den 22. december 2016

Deloitte
Statsautoriseret Revisionspartnerselskab



Ulrik Vassing
statsautoriseret revisor

Lars Holm Sørensen
partner, CISA