

Københavns Kommune
Koncernservice
Att.: Mikkel Hemmingsen
Borups Alle 177
2400 København NV

Revisionsrapport – Revision af generelle it-kontroller 2015

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2015 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 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 KMD's fælleskommunale systemer, KØR og Navision (i TMF), samt hvorvidt kontrollerne har fungeret i hele revisionsperioden vedrørende KMD's fælleskommunale systemer og 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 nedenstående 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 Navision (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, forventes gennemgået af Deloitte hos KMD i foråret 2016.

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 2015 og ved interview af relevant personale hos Københavns Kommune, samt ved observation, gennemgang af udleveret materiale og gennemgang af den tekniske sikkerhedsopsætning på udvalgt platform.

2. Ledelsesresume og konklusion

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


- Der er ikke foretaget en gennemgang af tildelte rettigheder til brugere i KSP-CICS (brugeradministrationsmodul), observation 3.2.

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	<p>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.</p> <p>Status 2015</p> <p>Vi har konstateret, at it-risikoanalysen er gennemført for <i>it-infrastruktur</i>.</p>	<p>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.</p>	<p>Vi skal anbefale, at it-risikoanalyserne gennemføres på de resterende og øvrige ansvarsområder, jf. kommunens plan herfor.</p>	●	

Organisationsområde i KK		Koncernservice (KS)	Revisionsområde/ emne	Generelle it-kontroller	
Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & væsentlighed	
3.2 Brugerrettigheder – periodiske revurdering (AD-KØR- KSP-CICS)	<p>Vi har konstateret, at der er etableret kørsler og rapporter, som kan benyttes til periodisk revurdering af tildelte rettigheder til KØR og AD'et.</p> <p>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.</p> <p>Status 2015</p> <p>Vi har noteret, at der som en del af ledelsestilsynet er udført review af brugerprofiler og tildelte adgange, hvorfor punktet lukkes.</p>	Manglende eller utilstrækkelig periodisk revurdering af tildelte rettigheder til brugere medfører risiko for, at brugeres rettigheder bliver utilstrækkelige og ikke afspejler deres arbejdsmæssige betingede behov.	<p>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.</p> <p>Ansvar herfor ligger i forvaltningerne for egne brugere.</p>		
3.2 Brugerrettigheder – Periodisk Revurdering (KSP-CICS)	<p>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.</p> <p>Kommunen har i januar 2016 afsluttet en revurdering af tildelte adgange til brugeradministration i KSP-CICS, som har givet anledning til enkelte justeringer og opfølgingspunkter.</p>	Manglende eller utilstrækkelig periodisk revurdering af tildelte rettigheder til brugere medfører risiko for, at brugeres rettigheder bliver utilstrækkelige og ikke afspejler deres arbejdsmæssige betingede behov.	<p>Vi skal henstille, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere for relevante systemer og platforme.</p> <p>Ansvar herfor ligger i forvaltningerne for egne brugere.</p>		

Organisationsområde i KK		Koncernservice (KS)	Revisionsområde/ emne	Generelle it-kontroller	
Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed	
	<p>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.</p>	<p>Manglende eller utilstrækkelig sikkerhedsmæssig logning medfører risiko for, at forsøg på uautoriserede handlinger ikke opdages og imødegås i tilstrækkeligt omfang.</p>	<p>Vi anbefaler, at der etableres en procedure for håndtering af logs, herunder en beskrivelse af logkrav, samt hvorledes der skal følges op på logs.</p> <p>Endvidere anbefaler vi, at systemejer formelt godkender denne logprocedure samt sikrer, at logproceduren er implementeret som vedtaget.</p> <p>Ydermere anbefaler vi, at periodisk gennemgang af relevante logs dokumenteres.</p>	●	
3.3 It-sikkerhedslogning (AD, KØR, TMF)	<p>Vi har dog konstateret, at der er etableret it-sikkerhedslogning på den reviderede Windows platform "Navision TMF Microsoft SQL" server.</p> <p>Endvidere har vi fået oplyst, at der ikke er etableret periodisk review af de logs, som på nuværende tidspunkt er etableret.</p> <p>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.</p> <p>Status 2015</p> <p>Vi har konstateret, at logningskrav fortsat ikke er formelt defineret for de tre områder inkluderet i denne revision.</p> <p>Det er endvidere oplyst, at logmanagement værktøjet LogPoint er implementeret, og at tre specialister, som skal hjælpe Københavns Kommune med håndtering af værktøjet, er rekrutteret. Kommunen forventer, at projektet vedrørende vurdering af logs samt procedure for gennemgang af disse vil blive gennemført i løbet af 2016.</p> <p>Yderligere har vi fået oplyst, at der er etableret en månedlig gennemgang af succesfulde loginforsøg til KØR databasen samt gennemgang af RDP logins til TMF serveren og anvendelse af SUPER-rollen.</p> <p>Der foreligger dog ingen dokumentation for gennemgangen af øvrige logs samt eventuelle affødte handlinger.</p>				

Organisationsområde i KK		Koncernservice (KS)	Revisionsområde/ emne	Generelle it-kontroller	
Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed	
3.4 Ændringskontrol – fallback (KØR)	<p>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.</p>	<p>Manglende eller utilstrækkelig planlægning af fallback medfører risiko for unødige komplikationer i forbindelse med, at fejlbehæftede ændringer implementeret i produktionsmiljøet forsøges fjernet igen.</p>	<p>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.</p>	●	
	<p>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.</p> <p>Det er dog oplyst, at det forventes, at KMD kan foretage en eventuel re-etablering til stadiet før implementeringen, såfremt ændringen medfører fejl.</p> <p>Status 2015</p> <p>Vi har konstateret, at forholdet er uændret, idet vi for 3 ud af 5 stikprøver ikke har modtaget dokumentation for fallback overvejelser.</p>				
3.5 Brugerrettigheder og funktionsadskillelse i TMF	<p>Vi har fået oplyst, at der ikke er foretaget formelle vurderinger af, hvorvidt der er etableret tilstrækkelig systemmæssig funktionsadskillelse i Navision.</p> <p>Status 2015</p> <p>Vi har konstateret, at der er en formel proces for godkendelse af rettigheder til Navision samt kontrol med anvendelsen af Super-rollen, som har fuld adgang til systemet.</p> <p>Der foreligger dog ingen formel proces til sikring af, at der ifm. tildelingen af adgange ikke tildeles konflikterende adgange, som udgør en risiko for omgåelse af øvrige interne kontroller.</p>	<p>Manglende eller svage procedurer vedrørende administration og vedligeholdelse af adgange til systemer medfører øget risiko for, at tildelte adgangsrettigheder overstiger brugerens arbejdsmæssige betingede behov eller ikke understøtter virksomhedens organisatoriske opdeling af arbejdsopgaver.</p>	<p>Vi anbefaler, at TMF foretager 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.</p>	●	

Organisationsområde i KK		Koncernservice (KS)	Revisionsområde/ emne	Generelle it-kontroller	
Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed	
3.6 Ændringskontrol – adgangskontrol til miljøer (TMF)	<p>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.</p> <p>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 driftsættelses-loggen.</p> <p>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.</p> <p>Status 2015</p> <p>Vi har fået oplyst, at de to personer fra Navision-gruppen med udviklerrettigheder er flyttet til 'Center for implementering og udvikling', således at der nu er etableret organisatorisk funktionsadskillelse. Det er oplyst, at disse ikke længere foretager udviklingsaktiviteter i Navision, men alene flytter ændringer fra test- til produktionsmiljøet. Derudover har vi konstateret, at der foretages en periodisk gennemgang af kritiske roller i Navision, herunder SUPER-rolle. Punktet lukkes.</p>	Manglende eller utilstrækkelig kontrol med udvikleres adgange til produktionsmiljøer medfører risiko for, at fejl eller ændringer utilsigtet introduceres i produktionsmiljøet.	<p>Vi skal anbefale, at "Application Builder" licensretigheden fjernes fra den applikationslicens, der anvendes på produktionssystemet. Derved vil der ske en reduktion i, hvad der kan ændres direkte i produktionsmiljøet.</p> <p>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.</p> <p>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.</p>		
3.7 Windows AD (TMF)-No Password Expiration	<p>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.</p> <p>Derudover har vi konstateret, at profilen KK\$ er undtaget fra brug af password.</p>	Manglende krav om periodisk skift af password for brugerprofiler medfører øget risiko for, at sådanne passwords med tiden bliver kendt af andre, hvormed sikkerheden på systemet kan blive kompromitteret.	<p>Vi anbefaler, at alle personlige brugerprofiler er forpligtet til at følge de overordnede krav om periodiske ændring af password.</p> <p>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.</p>		

Organisationsområde i KK		Koncernservice (KS)	Revisionsområde/ emne	Generelle it-kontroller	
Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed	
3.8 Windows AD (TMF) - Administrators	<p>Vi har konstateret, at 31 personlige brugerprofiler er tildelt Administratorrettigheder, og 77 brugerprofiler er medlemmer af brugergrupper med administratorrettigheder.</p> <p>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 administratorprofil eller medlemskab af brugergrupper, og som ikke alle længere har tilknytning til KS.</p>	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 periodisk 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

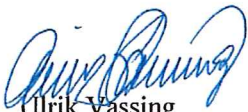
Nærværende rapport har i udkast været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

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 28. april 2016

Deloitte

Statsautoriseret Revisionspartnerselskab



Ulrik Vassing
statsautoriseret revisor



Lars Holm Sørensen
partner, CISA

