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
Økonomiforvaltningen
Att.: Adm. direktør Peter Stensgaard Mørch
Københavns Rådhus
1599 København V

Revisionsrapport – Revision af generelle it-kontroller 2017

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2017 har vi foretaget revision af de generelle it-kontroller, som understøtter kommunens regnskabsaflæggelse.

Rapporteringen er opbygget på følgende måde:

1. Formål, 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. Som en del af revisionen udvælges endvidere enkelte it-områder til den lovpligtige forvaltningsrevision.

Revisionens formål er dels at understøtte den lovpligtige forvaltningsrevision og dels at undersøge, om de generelle it-kontroller er udformet og implementeret på en hensigtsmæssig måde vedrørende KØR og Kvantum, samt om kontrollerne har fungeret i hele revisionsperioden vedrørende KØR og Kvantum.
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 væsentlige fejl i regnskabsaflæggelsen.

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. Revisionen har omfattet en vurdering af generelle kontroller inden for nedennævnte områder:

- 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 Kvantum.

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 KØR og Kvantum og tilhørende platforme. Der modtages årligt en revisionserklæring for de generelle it-kontroller omfattende KMD's generelle driftsydelser. Vi har af KMD's revisor fået bekræftet, at Kvantums infrastruktur er omfattet af KMD's generelle driftsydelser; dog anbefaler vi, at der fremadrettet indhentes en specifik revisionserklæring for Kvantum for at opnå en højere grad af sikkerhed. KMD's revisor har endvidere oplyst, at KØR ikke er omfattet af KMD's generelle driftsydelser, og at der ikke er afgivet en specifik erklæring for KØR. Der kan således være forhold og risici relateret til den generelle drift af KØR i 2017, som vi ikke bekendt med.

Forvaltningsrevisionen har omfattet en vurdering af igangsatte aktiviteter inden for nedennævnte områder:

- It-sikkerhedsregulativet
- Sikkerhedsprogrammet
- Risikovurderinger
- Sikkerhedsvurdering/ibrugtagningslister
- Beredskabsplaner.

It-sikkerhedsregulativet/sikkerhedsprogrammet og tilhørende risikovurderinger

Københavns Kommune fik i 2014 foretaget en ekstern vurdering af kommunens modenhed inden for it-sikkerhedsledelse og risikostyring. Det blev i modenhedsvurderingen konstateret, at it-sikkerhedsledelsen og risikostyringen i 2014 var mangelfuld på en række centrale områder. På baggrund heraf har Koncern-IT i 2017 udarbejdet et sikkerhedsprogram, som skal sikre medvirken til et generelt løft af it-sikkerhedsarbejdet i kommunen. I sikkerhedsprogrammet er der foreslået ni indsatsområder, som der arbejdes videre med i 2018.

Vi har endvidere konstateret, at kommunen har udarbejdet en indstilling til styrket IT governance på it- og persondataområdet, samt at IT governance-modellen trådte i kraft den 1. januar 2018 med en række initiativer, der skal etableres i løbet af 2018; der skal bl.a. gennemføres et risikovurderingsprojekt, hvor risikovurderinger udføres i et pilotforsøg med henblik på at gennemføre risikovurderinger i en mere færdig form i alle forvaltninger i 2018.

Det er vores vurdering, at der med it-sikkerhedsregulativet og sikkerhedsprogrammet er igangsat et omfattende arbejde, som har givet et generelt løft i it-sikkerheden i kommunen. Hvad angår pilotforsøget med risikovurderingsprojekt har vi konstateret, at skabelonen til risikovurderingen tager udgangs-

punkt i sikkerhedsområderne og definerer risici ud fra disse. Vi anbefaler, at der tages udgangspunkt i forretningsmæssigt vigtige (it-)aktiver og de dertil knyttede trusler/risici, og at det derudfra defineres, hvilke områder der er de vigtigste at prioritere.

Sikkerhedsvurdering/ibrugtagningslister

Som et led i den øgede fokus på it-sikkerhed har vi konstateret, at Koncern IT (KIT) har udarbejdet Sikkerhedsvurdering/ibrugtagningslister, der definerer, hvilke kriterier der ligger til grund for sikkerhedsvurderingen af nye it-systemer og infrastruktur. Sikkerhedsvurderingen foretages første gang, systemet meldes ind i FISKK, samt hver gang systemet efterfølgende skifter livscyklusfase.

Det er vores vurdering, at der med Sikkerhedsvurdering/ibrugtagningslister er designet og implementeret tilstrækkelige kontroller til at sikkerhedsvurdere nye it-systemer og infrastruktur.

Beredskabsplaner

Slutteligt som et led i forvaltningsrevisionen har vi gennemgået it-nedbruddet, som Københavns Kommune oplevede tilbage i oktober 2017, hvor størstedelen af kommunens it-systemer var utilgængelige. Vi har gennemgået beredskabsprocessen omkring it-nedbruddet og konstateret, at beredskabsorganisationen blev aktiveret efter planen. Vi har fået oplyst, at samtlige systemer var genetableret i løbet af 24 timer uden datatab. Den efterfølgende evaluering af beredskabsforløbet konkluderede, at krisen generelt blev håndteret tilfredsstillende; dog har evalueringen afstedkommet en række anbefalinger, herunder at der etableres ny organisering, hvor roller formaliseres, samt at der etableres et krisesekretariat, som skal assistere krise- og operationsledelsen med bl.a. kommunikation.

Vi vurderer, at der har været en tilstrækkelig proces vedrørende vurdering og evaluering af it-nedbruddet og beredskabsprocessen. Vi har konstateret, at kommunens evaluering har resulteret i et behov for en revurdering af beredskabsplanerne, og vi har konstateret, at dette arbejde er igangsat.

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 2017 og ved interviews af relevant personale hos Københavns Kommune samt ved observationer og stikprøvevis gennemgang af udleveret materiale.

2. Ledelsesresume og konklusion

It-revisionen har givet anledning til i alt 2 revisionsbemærkninger. Af de afgivne revisionsbemærkninger kan:

- 1 revisionsbemærkning henføres til en ny bemærkning i forbindelse med den udførte it-revision
- 1 revisionsbemærkninger henføres fra tidligere år til revisionen af årsregnskabet
- 2 revisionsbemærkninger fra tidligere år vurderes lukket i forbindelse med den udførte revision

2.1. Revisionserklæringer

Der modtages årligt en revisionserklæring for de generelle it-kontroller, omfattende KMD's generelle driftsydelser. Vi har af KMD's revisor fået bekræftet, at Kvantums infrastruktur er omfattet af KMD's generelle driftsydelser; dog anbefaler vi, at der fremadrettet indhentes en specifik revisionserklæring for Kvantum for at opnå en højere grad af sikkerhed. KMD's revisor har endvidere oplyst, at KØR ikke er omfattet af KMD's generelle driftsydelser, og at der ikke er afgivet en specifik erklæring for KØR. Der kan således være forhold og risici relateret til den generelle drift af KØR i 2017, som vi ikke bekendt med.

3. Observationer, risikovurdering og anbefaling

Observationer opdeles i henholdsvis:

1. Nye bemærkninger i forbindelse med den udførte it-revision (3.1)
2. Bemærkninger fra tidligere år og hvortil det vurderes, at disse videreføres i indeværende år (3.2)
3. Bemærkninger fra sidste år, der i forbindelse med it-revisionen er konstateret lukket (3.3)
4. Andre observationer (3.4).

3.1. Nye bemærkninger i forbindelse med den udførte it-revision

Organisationsområde i KK	Økonomiforvaltningen (ØKF)	**Revisionsområde/ emne**	Generelle it-kontroller og udvalgte områder til forvaltningsrevision

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko & Væsentlighed**
3.1.1 Revisionserklæringer	Københavns Kommune har indgået aftale med KMD omkring drift af KØR og Kvantum og tilhørende platforme. Der modtages årligt en revisionserklæring for de generelle it-kontroller, omfattende KMD's generelle driftsydelser. Vi har af KMD's revisor fået bekræftet, at Kvantums infrastruktur er omfattet af KMD's generelle driftsydelser. Dog henstiller vi, at der indhentes en specifik revisionserklæring for Kvantum for at opnå en højere grad af sikkerhed. KMD's revisor har endvidere oplyst, at KØR ikke er omfattet af KMD's generelle driftsydelser, og at der ikke er afgivet en specifik erklæring for KØR. Der kan således være forhold og risici relateret til den generelle drift af KØR i 2017, som vi ikke bekendt med.	En manglende eller utilstrækkelig overvågning af underleverandører medfører risiko for, at underleverandører ikke efterlever det forventede it-sikkerhedsniveau.	Vi henstiller, at der indhentes specifikke revisionserklæringer vedrørende KMD's drift af Kvantum og KØR. Det er oplyst, at Københavns Kommune har anmodet KMD om en specifik erklæring på Kvantum, ligesom det er aftalt, at der tilvejebringes den nødvendige erklæring vedrørende KØR, som efter det oplyste vil foreligge inden afgivelse af revisionsberetningen for 2017.	

3.2. Bemærkninger fra tidligere år og hvortil det vurderes, at disse videreføres i indeværende år

Organisationsområde i KK	Forvaltningerne	**Revisionsområde/ emne**	Generelle it-kontroller og udvalgte områder til forvaltningsrevision

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko & Væsentlighed**
3.2.1 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 bestyrelsens godkendelse. KK forventer, at risikoanalyser for de enkelte forvaltninger udarbejdes i løbet af 2015. **Status 2017** Vi har konstateret, at KK i 2017 har iværksat en proces med henblik på vurdering samt udvælgelse af fagsystemer, som skal indgå i det påbegyndte risikovurderingsprojekt, hvor fokus primært er systemer, som indeholder personfølsomme data. De gennemførte risikovurderinger er udført i et pilotforsøg med henblik på at gennemføre risikovurderinger i en mere færdig form i alle forvaltninger i 2018, herunder it-infrastruktur.	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 henstiller, at forvaltningerne tilvejebringer den nødvendige dokumentation, og at KIT snarest herefter gennemfører it-risikovurderingerne i overensstemmelse med kravene i it-sikkerhedsregulativet, og at de gennemføres snarest muligt.	

3.3. Bemærkninger fra sidste år, der i forbindelse med it-revisionen er konstateret lukket

Organisationsområde i KK	Økonomiforvaltningen (ØKF)	**Revisionsområde/ emne**	Generelle it-kontroller og udvalgte områder til forvaltningsrevision

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko & Væsentlighed**
3.3.1 Sikkerhed kontinuerlig overvågning	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 log management-værktøjet LogPoint er implementeret, og at 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. **Status 2017** Vi har konstateret, at der nu er etableret en centraliseret løsning af log management. Logdata opsamles i kommunens centrale SIEM-system, hvorfra der på baggrund af en automatiseret proces sker rapportering af udvalgte hændelser. Punktet lukkes.	Manglende eller utilstrækkelig sikkerhedsmæssig logning medfører risiko for, at forsøg på uautoriserede handlinger ikke opdages og imødegås i tilstrækkeligt omfang.	Vi henstiller, 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.	
3.3.2 Datasikkerhed	Vi har fået oplyst, at datatransport for så vidt angår persondata og værdidata altid skal foregå ved krypteret trafik, og at data på fysiske diske og USB (beskyttet med password) sendes med personlig overdragelse, og at der indhentes kvittering for modtagelse. Endvidere har vi observeret, at der ikke sker nogen systematisk opfølgning på, om medarbejdere i modstrid med reglerne opbevarer persondata på bærbare computere, og at data på disse computere ikke er krypteret. Endelig er det konstateret, at der hidtil ikke har foreligget retningslinjer for styring af mobile enheder (telefoner og tablet), men at sådanne retningslinjer, startende i oktober 2015, er under indførelse i forbindelse med det såkaldte "AirWatch-projekt".	En manglende eller utilstrækkelig datasikkerhed medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at projektet vedrørende implementering af Windows 10 Enterprise fortsættes og gennemføres efter planen.	

	Vi har endvidere konstateret, at der er implementeret en procedure for bortskaffelse af informationsbærende medier, samt at der er igangsat et projekt, hvor Windows 7 skal udskiftes med Windows 10, og i den forbindelse vil harddiske blive krypteret. For mobile enheder er AirWatch etableret, og der er udarbejdet formelle retningslinjer. **Status 2017** Størstedelen af tidligere rapporteret forhold vurderes lukket. Der er dog enkelte udestående tilbage, som er rapporteret under andre bemærkninger ref. punkt 3.9.			

3.4. Andre observationer

Organisationsområde i KK	Forvaltningerne	Revisionsområde/ emne	Generelle it-kontroller og udvalgte områder til forvaltningsrevision

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed
3.4.1 Beredskabsplaner	Vi har konstateret, at it-beredskabsplanen for KK ikke har været opdateret siden 2015. Dette begrundes med, at KK har sat opdateringsarbejdet af beredskabsplanen i bero, da overvejelser af, hvilke tiltag der skal tages for at styrke og omorganisere beredskabsplanen, er igangværende. Derudover er det oplyst, at KK i 2017 har haft fokus på udarbejdelse af beredskabsplaner i de enkelte forvaltninger. Projektet er igangværende og således ikke fuldført.	En manglende eller utilstrækkelig it-beredskabsplan medfører risiko for, it-systemer ikke kan etableres som forventet i tilfælde af en sikkerhedshændelse.	Vi henstiller, at grundlaget for og formålet med beredskabsplanlægningen for de enkelte forvaltninger fastlægges og godkendes formelt af ledelsen, samt at opfyldelsen af kravene pr. system og platform efterfølgende dokumenteres og rapporteres til ledelsen. Yderligere anbefaler vi, at beredskabsplaner opdateres periodisk - minimum en gang årligt samt når andre faktorer indikerer nødvendigheden heraf.	

Organisationsområde i KK	Økonomiforvaltningen (ØKF)	Revisionsområde/ emne	Generelle it-kontroller og udvalgte områder til forvaltningsrevision

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko & Væsentlighed
3.4.2 It-sikkerhedspolitik og it-sikkerhedsregler	Vi har konstateret, at KK's it-sikkerhedspolitik samt underliggende, uddybende it-sikkerhedsregler ikke er gennemgået og reviewet siden 2013. Det er yderligere oplyst, at sikkerhedspolitikker er planlagt til revidering i Q1 2018.	Et manglende eller utilstrækkeligt it-sikkerhedspolitik medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at it-sikkerhedspolitikken samt de underliggende it-sikkerhedsregler revurderes periodisk - som minimum årligt samt ved væsentlige ændringer i risikobilledet.	

3.4.3 Sikkerhedsprogram	PwC har i 2014 vurderet, at Københavns Kommunes modenhed på daværende tidspunkt var mangelfuld på en række centrale områder. I en opfølgende måling i 2016 er det vurderet, at der er sket en øget modenhed på de områder, hvor der er gennemført særlige tiltag, men at der samtidig var en del forbedringspunkter. På baggrund heraf har Københavns Kommune udarbejdet et sikkerhedsprogram, som skal medvirke til et generelt løft af it-sikkerhedsarbejdet i kommunen. Der bliver i sikkerhedsprogrammet foreslået ni indsatsområder, som der arbejdes videre med, enten som allerede igangsatte tiltag eller organiseret som nye projekter.	Et manglende eller utilstrækkeligt it-sikkerhedsprogram medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at arbejdet med indsatsområder i sikkerhedsprogrammet fortsættes og gennemføres efter planen 1) Ansvarsfordeling 2) Revision af sikkerhedsregulativet 3) It-sikkerheds-processer og værktøjer 4) Oprydning på fællesdrev 5) Samlet program for uddannelse 6) Risikovurdering/styring 7) Incidenthåndtering 8) Opfølgning på loghændelser 9) Tilsyn	

3.4.4 IT-governance	I revisionsrapport for 2016 påpeger Intern Revision (IR), at der reelt mangler governance på it-området. IR anbefaler: • At governance skal fastlægges i en række standardiserede styringsregler og retningslinjer for anskaffelser • At der sker en entydig placering af beslutningsansvaret som en integreret del af kommunens strategiske ledelsesarbejde • At der arbejdes med en risikobaseret tilgang til styring af it-sikkerhed og IT governance • At der etableres en it-kreds til håndtering af den ledelsesmæssige forankring. Det er her afgørende, at topledelsen er repræsenteret i kredsen. Vi har i forbindelse med vores revision 2017 konstateret, at kommunen har udarbejdet en indstilling til styrket IT governance på it- og persondataområdet, samt at IT governance-modellen trådte i kraft den 1. januar 2018 med en række initiativer, der skal etableres i løbet af andet halvår 2018: • Etablering af en it-kreds på tværs af kommunens forvaltninger • Tværgående strategier • Klar rolle- og ansvarsfordeling i it-anskaffelsesprocesser Vi er informeret om, at it-kredsens arbejdsprogram vil blive forelagt kredsen af administrerende direktører til godkendelse i 1. kvartal 2018. Et cirkulære for it-anskaffelser i KK forelægges for ØU i 2. halvår 2018. Cirkulæret erstatter den gældende anskaffelsesvurderingsproces fra 2012. En samlet redegørelse med fokus på varetagelse af it-sikkerhedsområdet forelægges for ØU og BR ved udgangen af 1. halvår 2018. Der udarbejdes en samlet status på it-kredsens arbejde i slutningen af 2018 til forelæggelse for ØU.	En manglende eller utilstrækkelig governance på it-området medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at arbejdet med en styrket IT governance-model forsættes og gennemføres efter planen	

3.4.5 Datasikkerhed	Vi har fået oplyst, at datatransport for så vidt angår persondata og værdidata altid skal foregå ved krypteret trafik, og at data på fysiske diske og USB (beskyttet med password) sendes med personlig overdragelse, og at der indhentes kvittering for modtagelse. Endvidere har vi observeret, at der ikke sker nogen systematisk opfølgning på, om medarbejdere i modstrid med reglerne opbevarer persondata på bærbare computere, og at data på disse computere ikke er krypteret. Endelig er det konstateret, at der hidtil ikke har foreligget retningslinjer for styring af mobile enheder (telefoner og tablet), men at sådanne retningslinjer, startende i oktober 2015, er under indførelse i forbindelse med det såkaldte "AirWatch-projekt". Vi har endvidere konstateret, at der er implementeret en procedure for bortskaffelse af informationsbærende medier, samt at der er igangsat et projekt, hvor Windows 7 skal udskiftes med Windows 10, og i den forbindelse vil harddiske blive krypteret. For mobile enheder er AirWatch etableret, og der er udarbejdet formelle retningslinjer. **Status 2017** Vi har fået oplyst, at implementering af Windows 10 Enterprise med Bitlocker er påbegyndt i februar 2018 og forventes afsluttet omkring Q3 2018. Herved vil kommunen sikre kryptering af alle harddiske.	En manglende eller utilstrækkelig datasikkerhed medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at projektet vedrørende implementering af Windows 10 Enterprise fortsættes og gennemføres efter planen.	

3.4.6 It-risikoanalyse - Kvantum	Vi har konstateret, at KK i 2017 har iværksat en proces med henblik på vurdering og udvælgelse af fagsystemer, som skal indgå i det påbegyndte risikovurderingsprojekt, hvor fokus primært er på systemer, som indeholder personfølsomme data. Desuden er det konstateret, at det nye Kvantum-system ikke har været omfattet af udvalgte systemer. Det er endvidere oplyst, at der i forbindelse med idriftsættelse af systemet i 2017 er udarbejdet ibrugtagningstilladelse, hvori systemet er godkendt på baggrund af en overordnet risikovurdering. Prioritering vil være gul for denne.	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 henstiller, at Kvantum indgår i risikovurderingsprojektet, så der sikres en løbende opfølgning på risikobilledet i forhold til Kvantum.	

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

- Prioritet 3-markeringer 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 Lars Kronow på telefon 2220 2786 eller Jesper Due Sørensen på telefon 30 93 64 20.

København, den 19. april 2018

Deloitte
Statsautoriseret Revisionspartnerselskab

Lars Kronow
statsautoriseret revisor

Jesper Due Sørensen
partner

c.c.: Københavns Kommune Koncernservice, Irene Ludvigsen

JHON/ach/as/ABP
T:\Afd1180\Københavns Kommune 154164\2018\Københavns Kommune GIK-rapport END 190418_2.docx