Bilag 2 – Revisionsbemærkninger med tilføjet handleplan og status

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	København 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 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.	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.		**Handleplan og status for Revisonserklæringer** Revisorerklæring for Kvantum er under indhentning fra KMD. Revisorerklæring for KØR er under indhentning fra Deloitte. Begge erklæringer vil foreligge inden afgivelse af revisionsberetningen for 2017, så observationen forventes at gå i grønt.

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 fået oplyst, 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. Yderligere er det oplyst, at det nye Kvantum-system ikke har været omfattet af udvalgte systemer.	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 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.		**Handleplan og status for It-risikoanalyse** På baggrund af erfaringerne fra risikovurderingerne i 2017 er der foretaget en række justeringer ift. risikokonceptet for 2018. KIT vil i den forbindelse, dels adressere spørgsmålet om manglende dokumentation over for forvaltningerne, dels gennemføre risikovurderinger i videst muligt omfang til trods for en eventuel mangel på dokumentation. KIT færdiggør pt. alle standarddokumenter til brug for risikovurderingerne 2018. Konceptet for risikovurderinger præsenteres for DCK og It-kredsen ultimo 2. kvartal 2018. Forvaltningerne kontaktes i løbet af maj med henblik på tilrettelæggelse af forløbet, hvorefter risikovurderingerne i praksis gennemføres henover sommer og efteråret. Efter udarbejdelse af risikovurderinger for de enkelte forvaltninger og den samlede risikovurdering for kommunen orienteres DCK, ØU og BR om kommunens samlede risikobillede med henblik på, at BR i sidste ende træffer beslutning om kommunens overordnede it-sikkerhedsniveau.

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.		**Handleplan og status for Beredskabsplaner** Udkast til ny *overordnet beredskabsplan* for KK forventes at være klar ultimo maj 2018 med henblik på involvering af interessenter. KIT forventer endvidere at kunne præsentere den endelige reviderede beredskabsplan i slutningen af 3. kvartal. I forhold til *forvaltningsspecifikke beredskabsplaner* er der udarbejdet et paradigme med angivelse af specifikke krav til en sådan beredskabsplan. KIT gennemførte i 2017 tilsyn med it-sikkerheden i kommunens forvaltninger: Denne viste, at én forvaltning har en færdig it-beredskabsplan, og at én forvaltning delvist har en it-beredskabsplan. Fem forvaltninger har ikke tilgængelige it-beredskabsplaner. Arbejdet er i gang og der er fastsat deadlines. I tilknytning til ovenstående planlægger KIT en *kriseøvelse*, som vil blive tilrettelagt og gennemført i samarbejde med Hovedstadens Beredskab. Formålet med øvelsen er primært at teste den praktiske anvendelse af beredskabsplaner, herunder navnlig at træne kommunikationen og samarbejdet mellem forvaltningerne. Selve øvelsen forventes umiddelbart afviklet i oktober 2018. Endelig udarbejder KIT en *genopretningsplan* for de kritiske it-systemer i KK. Planen baserer sig på en analyse af KK's tekniske cyberforsvar, som Deloitte i samarbejde med KIT afleverer primo maj 2018. Den endelige genopretningsplan vil herefter blive forelagt It-kredsen og efterfølgende til 7-DIR til endelig godkendelse.

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.		**Handleplan og status it-sikkerhedspolitik og -regulativ** Københavns Kommunes It- sikkerhedsregulativ er senest ændret d. 2. februar 2017 for at adressere større organisatoriske ændringer i kommunen og for at give Økonomiforvaltningen mulighed for at udarbejde cirkulærer fremadrettet. Ved samme lejlighed fik kommunens bindende retningslinjer status af cirkulærer. Pt. foretages en gennemgribende revision af kommunens it-sikkerhedsregulativ og -politik, som forventes forelagt ØU og BR i første halvår 2018. Regulativ vil bl.a. beskrive kommunens DPO-funktion. I dialog med intern revision er der planlagt udarbejdelse af seks cirkulærer i medfør af Informationssikkerhedsregulativet: Databeskyttelse, Organisering af informationssikkerhed, Informationssikkerhedsregler, It-anskaffelse, It-drift og vedligehold, It-afvikling/udfasning. Cirkulærer vedr. informationssikkerhedsregler og it-anskaffelse fremlægges for ØU i 2. halvår 2018. I 2. halvår 2018 udarbejdes en bølgeplan for udarbejdelse af øvrige cirkulærer, dvs. for databeskyttelse, organisering af informationssikkerhed, it-drift og vedligehold, it-afvikling/udfasning samt understøttende forretningsgange. Den konkrete udarbejdelse af cirkulærer og forretningsgange vil strække sig over andet halvår 2018 og ind i første halvår 2019.

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-sikkerhedsprocesser og værktøjer 4) Oprydning på fællesdrev 5) Samlet program for uddannelse 6) Risikovurdering/styring 7) Incidenthåndtering 8) Opfølgning på loghændelser 9) Tilsyn		**Handleplan og status for Sikkerhedsprogrammet** Sikkerhedsprogrammet i Koncern IT (KIT) har i tæt samarbejde med LCP-programmet til formål at koordinere informationssikkerhedsaktiviteter med henblik på at højne kvaliteten af arbejdet med informationssikkerhed i hele Københavns Kommune. Grundlaget for sikkerhedsprogrammet blev forelagt Økonomikredsen i marts 2017 og forventes afsluttet i juni 2018. 1) Ansvarsfordeling er afsluttet medio 2017 2) Revision af sikkerhedsregulativet er under udarbejdelse, jf. 3.4.2 3) It-sikkerhedsprocesser og værktøjer er afsluttet medio 2017 4) Oprydning på fællesdrev følger den forvaltningsspecifikke plan for overgangen til Office 365, der afsluttes ultimo 2018 5) Samlet program for uddannelse er godkendt af ØK, og uddannelse i de enkelte forvaltninger forventes afsluttet ultimo september 2018 6) Risikovurdering/styring er i proces, jf. 3.2.1 7) Incidenthåndtering (sikkerhedshændelser) er under udarbejdelse og forventes afsluttet ultimo maj 2018 8) Opfølgning på loghændelser: Kortlægningen af relevante fagsystemer afsluttes ultimo maj 2018, hvorefter implementeringsprojektet igangsættes. 9) Tilsyn med forvaltningerne er afsluttet primo april 2018 med oversendelse af samlet afrapportering til intern revision.

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		**Status for IT-governance** Der er etableret en It-kreds på direktørniveau (samt Databeskyttelsesrådgiveren, DPO) og udarbejdet et arbejdsprogram for It-kredsen for 2018. Heri indgår, at der i Q3 2018 udarbejdes fælles strategier for infrastruktur, rammearkitektur, fællessystemer og it-sikkerhed. Der er endvidere igangsat initiativer vedr. opdatering af kommunes regelsæt på informationssikkerhedsområdet, jf. pkt. 3.4.2. En samlet redegørelse med fokus på varetagelse af it-sikkerhedsområdet forelægges ØU og BR i løbet af 2018. Der udarbejdes en samlet status på It-kredsens arbejde i slutningen af 2018. Med nedsættelse af It-kredsen og udarbejdelsen af kredsens arbejdsprogram, er det KIT's opfattelse, at en styrket it-governancemodel er færdig-implementeret.

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.		**Handleplan og status for datasikkerhed** Der er iværksat et projekt, hvor samtlige pc'er på Københavns Kommunes administrative netværk enten opgraderes fra Windows 7 til Windows 10 eller udskiftes med nye pc'er med Windows 10. I denne forbindelse installeres også Office 365 på alle pc'er og alle harddiske krypteres. Der i alt ca. 20.700 aktive pc'er på kommunens administrative netværk. KIT har pt. udrullet Windows 10 på ca. 12.000 pc'er. Der opdateres/udskiftes pt. ca. 500 pc'er om ugen. Opdatering og udskiftning af de resterende ca. 8.700 pc'er sker fra medio maj 2018 til ultimo Q3 2018.

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.		**Handleplan og status for It-risikoanalyse - Kvantum** Der er i forbindelse med idriftsættelse af Kvantum blevet udarbejdet en ibrugtagningstilladelse, hvorved der er foretaget en overordnet risikovurdering. KIT vil i sit fremadrettede arbejde på risikoområdet sikre en løbende opfølgning på risikobilledet i forhold til Kvantum.