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 Søren Hartmann Hede
Københavns Rådhus
1599 København V

Revisionsrapport – Revision af generelle IT-kontroller 2020

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2020 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
5. Afslutning.

Sammenfatning

På baggrund af revisionen er det vores vurdering, at de af de generelle IT-kontroller, som vi har vurderet relevante for at understøtte revisionen af årsrapporten for Københavns Kommune i al væsentlighed har været hensigtsmæssigt udformet og opretholdt i revisionsperioden.

Der er i indeværende revisionsperiode sket et fald i antallet af revisionsbemærkninger for de reviderede områder. Faldet i revisionsbemærkninger kan henføres til udbedring af én revisionsbemærkning i forbindelse med revisionen af de generelle IT-kontroller samt tre revisionsbemærkninger vedrørende de gennemførte forvaltningsrevisioner. Endvidere er én revisionsbemærkning fra 2019 nedprioriteret til gul (prioritet 2).

Endvidere er det vores vurdering, at Københavns Kommune bør arbejde videre med implementeringen af en centraliseret løsning til udførelse af periodisk revurdering af brugere samt tildelte rettigheder i kommunens systemer.

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 Kvantum, KMD Opus Debitor, KMD Opus Løn og KMD Aktiv, samt om kontrollerne har fungeret i hele revisionsperioden.

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 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.

Lovpligtig revision
Revisionen er tilrettelagt således, at ikke alle områder gennemgås hvert år; dog således, at alle for regnskabet væsentlige områder bliver gennemgået samt væsentlige kontrolsvagheder altid bliver fulgt op ved efterfølgendes års revision. Revisionen har omfattet en vurdering af generelle IT-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
- Logisk sikkerhed: Fokus er på den logiske adgangsvej til systemerne, herunder password og styring af brugerprofiler
- Change management: Processer for vedligeholdelse af Kvantum, KMD Opus Debitor, KMD Opus Løn og KMD Aktiv.

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 Kvantum, KMD Opus Debitor, KMD Opus Løn og KMD Aktiv samt tilhørende platforme.

Der modtages årligt en revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser samt en årlig specifik erklæring til Kvantum.

Forvaltningsrevision
Forvaltningsrevisionen har omfattet en opfølgning af observationer fra revisionen af 2019 inden for nedennævnte områder:

- KIT's nye koncept for risikovurderinger
- Governance-modellen for anvendelse af SIEM
- Governance-modellen for udvikling og drift af robotter/automatiserede processer

- Overordnet gennemgang af BUF IT-drift
- Leverandørstyring
- SharePoint.

I følgende afsnit har vi beskrevet vores revision og opfølgning af de seks udvalgte forvaltningsområder.

KIT's koncept for 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 (herefter KIT) i 2017 fået til opgave at stå for processen til udarbejdelse af nye IT-risikovurderinger i Københavns Kommune. Som et led i Deloittes revision i 2020 har vi fulgt op på KIT's koncept for risikovurderinger.

Vi har konstateret, at koncept for IT-risikovurderinger har indarbejdet et trusselskatalog samt et katalog over sikringsforanstaltninger, som er gennemgået for de mest kritiske systemer, hvor der er udarbejdet en risikoanalyse. Det er vores vurdering, at trusselskataloget og kataloget over sikringsforanstaltninger har givet et godt fundament til udarbejdelsen af risikovurderinger.

Yderligere har vi konstateret, at de udarbejdede risikoanalyser har fået større ledelsesforankring på KK-niveau.

Endvidere har vi konstateret, at det udestår, at forvaltningerne får lukket de af KIT fremsatte henstillinger vedrørende risikovurderingerne for 2019.

Det er i forbindelse med 2020 revisionen, at koncern IT tilbage i 2019 har risikovurderet 61 af kommunens IT-systemer på tværs af forvaltningerne. Processen for udvælgelsen af systemer starter ved, at der årligt udarbejdes en indstilling til digitaliseringschefkredsen, hvori de overordnede rammer og fokusområder for årets risikovurderinger præsenteres og godkendes. Deloitte har konstateret, at KIT i fællesskab med DPO'en har udvalgt følgende 3 udvælgelseskriterier i 2020:

- Systemer, der behandler persondata
- Systemer, der behandler værdioplysninger
- RPD- og RDA-systemer.

Dernæst fremsendes kriterierne til forvaltningerne, således at de kan udvælge relevante systemer til den årlige risikovurdering.
Vi har for en stikprøve konstateret, at forvaltningerne fremsender en liste over de systemer, som findes relevante for årets risikovurderinger på baggrund af førnævnte udvælgelseskriterier. Ved modtagelse af relevante systemer foretages en kvalificering af KIT for at sikre, at alle relevante systemer er medtaget. På baggrund af den beskrevne proces har KIT i samråd med forvaltninger vurderet, at der i 2019 var 61 relevante IT-systemer på tværs af forvaltninger.

Resultatet heraf gav anledning til, at forvaltningerne i alt fik 146 henstillinger og 332 anbefalinger.

Det er konstateret, at de enkelte forvaltninger pr. august 2020 har nedbragt antallet af henstillinger og anbefalinger således, at 47 af 146 henstillinger samt 97 af 332 anbefalinger er efterlevet på tværs af forvaltningerne. Vi kan konstatere, at KIT's risikovurderinger laves årligt og dermed vil der tilkomme nye henstillinger og anbefalinger, som forvaltningerne skal have fokus på at lukke. Endvidere kan vi konstatere, at der pr. august 2020 var 3 systemer hos BUF, som skulle risikovurderes på ny grundet større ændringer. Re-risikovurdering er foretaget og afrapporteret pr. december 2020, hvormed de 3 systemer hos BUF ikke længere udestår.

Vi kan dermed konstatere, at KIT's koncept for risikovurderinger er fuldt implementeret.

Governance-modellen for anvendelse af SIEM

Københavns Kommunes SIEM-løsning blev anskaffet i april 2015 som en del af en flerårig indsats med fokus på at styrke IT-sikkerheden i Københavns Kommune. Anskaffelsen lå i forlængelse af PwC's modenhedsanalyse fra 2014 på IT-sikkerhedsområdet, der viste et markant forbedringspotentiale generelt på IT-sikkerhedsområdet. I analysen blev især manglende overvågning og logning af kommunens IT-aktiviteter fremhævet, hvorfor Security Information and Event (SIEM) overvågningsværktøjet blev anskaffet som en investering. Implementering af SIEM-løsningen blev gennemført i andet halvår 2015. Med virkning fra 1. januar 2016 blev der i KIT's sikkerhedskontor ansat et særligt monitoreringsteam til opbygning af den nye funktion. Efter en række tekniske tilpasninger har SIEM-systemet siden ultimo 2017 været i stabil drift.

Som et led af revisionen i 2020 har Deloitte fulgt op på tidligere rapporterede observationer vedrørende anvendelse af SIEM.

Vi har fået oplyst, at SIEM-løsningen anvendes til logning af systemer samt grundlæggende infrastrukturen. Netværk er logget på switchniveau. Endvidere er det oplyst, at der på domain controllers er opsat logning af alle log ind og -ud forsøg samt hvilken maskine, der arbejdes på. Desuden er 16 virtuelle firewalls logget i SIEM.

Efter det oplyste er der som udgangspunkt opsat logning på alle fagsystemer ud fra en "comply and explain model", som betyder, at der skal gives saglig begrundelse for at et fagsystem ikke medtages i logningen, f.eks. at systemet har en indbygget logningsløsning eller hvis der er ekstremt få brugere. Når logningen opsættes, inddrages systemejerne (teknisk og forretningsmæssigt) for fastsættelse af use-cases, som er meningsfulde at logge og anvende til rapportering.
Et system kan undtages for tilkobling til den centrale SIEM løsning, hvormed det vil være systemejernes ansvar at gennemføre en manuel logopfølgning.
Som udgangspunkt, har Københavns Kommune opsat en række standard use-cases for logopfølgning, som minimum skal implementeres, hvis det er teknisk muligt på alle SIEM integrerede fagsystemer:

1) ved tilføjelser eller fjernelser fra AD grupper
2) ved fejlede loginforsøg
3) ved unormale logintidspunkter og
4) ved opslag på/udbetaling til nære relationer.

Rapportering udsendes automatisk til systemejerne via e-mail, hvor systemejer modtager en ugentlig rapport samt alarmer i tilfælde af en hændelse.

Deloitte har i forbindelse med opfølgningen konstateret, at der i udvælgelsesprocessen af fagsystemer og infrastruktursystemer tages udgangspunkt i det samlede overblik, som er registreret i FISKK, hvor der tilbage i 2019 blev konstateret 986 systemer. Der står beskrevet i KK's uddybende IT-sikkerhedsregler, at forvaltningerne er forpligtet til at udføre logopfølgning, hvorfor der er blevet trukket en liste fra FISKK på tværs af forvaltningerne med fokus på systemer med personfølsomme data eller værdidata. Denne vurdering mindskede antallet til 267 systemer.
Efterfølgende er systemerne blevet gennemgået af forvaltningerne, således at systemer under udfasning eller som alligevel ikke indeholdt følsomme persondata eller værdidata blev valgt fra, hvilket gav en yderligere reduktion til 166 relevante systemer.
Igennem vurderingsmøder, hvor de relevante systemer blev drøftet, endte det med, at der totalt set blev udvalgt 36 systemer, som var teknisk egnede til at blive integreret i SIEM.

Det er oplyst, at der løbende igennem anskaffelsesprocessen, tilføjes nye fagsystemer til SIEM-porteføljen, når det er teknisk muligt.

I forlængelse heraf har Deloitte modtaget den afsluttende rapportering på logopfølgningsprojektet (20. februar 2020). Vi kan heri konstatere, at der løbende vedligeholdes en oversigt over fagsystemer, der skal integreres i SIEM-løsningen. Endvidere kan vi konstatere, at 32 ud af 36 udvalgte fagsystemer og

infrastruktursystemer, som forvaltningerne har udvalgt, og som KIT vurderede teknisk egnet, nu logges, samt at de resterende 4 har en saglig begrundelse for undtagelse fra logning. Desuden beskrives standard use-cases, ugentlige rapporter og alarmer samt overgangen til drift, hvor KIT har gennemgået nye logopfølgningsregler med alle forvaltninger.
På baggrund heraf har vi stikprøvevist gennemgået use-case-eksempler på KMD Aktiv samt Kvantum for at efterteste, hvorvidt implementeringen heraf er testet og godkendt forud for idriftsættelsen. Dette har ikke givet anledning til bemærkninger.

Endvidere har vi stikprøvevist gennemgået eksempler den gennemførte opfølgning på udløste alarmer, hvilket ikke har givet anledning til bemærkninger.

Samtidigt kan vi konstatere, at KIT har implementeret risiko awareness uddannelse for alle systemejere i KK. Det skyldes efter det oplyste, at det derved sikrer en bedre og mere kontinuerlig fokus på risiko og uddannelse end enkeltstående workshops om emnet.

Vi kan dermed konstatere, at projektet er afsluttet og fuldt implementeret.

Governance-modellen for udvikling og drift af robotter/automatiserede processer

Som et led i IT-revisionen (forvaltningsrevision) for 2020 har vi fulgt op på tidligere rapporterede forhold vedrørende Københavns Kommunes governance for udvikling og drift af robotter/automatiserede processer.

I relation til udviklingsfasen organiseres projekterne i en styregruppe og et kerneteam. Styregruppen består af procesejeren, ejeren af Robotics Process Automation (CoE) i kommunen og leveranceansvarlige. Det er i styregruppen, at beslutninger om de rette projektdeltagere, økonomi og ændringer til forretnings-/robotprocessen træffes. Kerneteamet står for det udførende samarbejde i projektet, hvor kombinationen af forretningens fagproceskendskab og RPA-leverandørens proceskonsulent/-udvikler kortlægger, designer og udvikler robottens arbejde.

I forbindelse med den daglige drift af robot-kørslerne har KIT RPA en fuldtidsoperatør. Det er dennes opgave at sikre, at alle robotter kører, som de skal, og efter de aftalte tider i driftsaftalerne. Til administration og overvågning af robot-kørslerne benyttes værktøjet UiPath. Ved fejl i kørslerne er det operatørens opgave at foretage fejlfinding. Der skelnes imellem to typer af fejl:

- Applikationsfejl
- Forretningsfejl eller undtagelse for forretningsregler.

Applikationsfejl er den type fejl, som et systemnedbrud f.eks. ville forårsage. Det er KIT RPA's opgave at rette disse typer af fejl, og hvis sådan en fejl har resulteret i fejlagtig sagsbehandling, er det KIT RPA's opgave at rette henvendelse til forvaltningen, så de kan rette op på den eller de pågældende sager.

Ved forretningsfejl er der i stedet tale om fejl, som man ved kan opstå under sagsbehandlingen, og som vil resultere i, at man behandler sagen anderledes end hovedparten af sagerne. Det er forvaltningernes ansvar at overvåge og håndtere forretningsfejl.

På baggrund af vores opfølgning af tidligere rapporterede forhold samt stikprøvekontrol kan vi konstatere, at Københavns Kommune har iværksat udbedrende aktiviteter, således har vores stikprøvegennemgang ikke givet anledning til bemærkninger.

For implementering af robotter før KIT overtog styringen i forbindelse med kontroller omkring implementeringen, har vi konstateret, at disse løbende opdateres og i den forbindelse gennemgår governance modellen.

BUF IT-drift

Forvaltningsrevisionen af BUF IT-drift omfattede i 2019 en overordnet gennemgang på interview basis af BUF IT-drift (herefter BIT) ydelser, herunder en vurdering af, hvorvidt KK's IT-retningslinjer er implementeret hos BIT.

BUF IT-drift er Børne- og Ungdomsforvaltningen i Københavns Kommunes IT-afdeling, der har til opgave af administrere, drifte og supportere IT på skoler og en række institutioner.

BIT's samlede ydelser består af en række fællesydelser og bestillingsydelser samt understøttelse af tekniske og administrative opgaver til omkring 72 skoler, hvor fokus er undervisningsudstyr til 0-18 års området.

BIT råder over omkring 50 medarbejdere, hvor af 21 er udkørende teknikere, som blandt andet varetager driftssupport.

Yderligere er det oplyst, at BIT på lige fod med de øvrige forvaltninger er underlagt KK's IT-sikkerhedspolitikker, regulativer samt cirkulærer. I forbindelse med ændringer og/eller opdateringer informeres BIT igennem digitaliseringschefen, og teamlederen i BIT sikrer, at disse kommunikeres til relevante medarbejdere.

BIT-medarbejdere har adgang til de selvbetjeningsløsninger, som KS tilbyder, og er ligeledes underlagt de obligatoriske awareness- samt e-learningsprogrammer.
Under vores gennemgang er vi blevet informeret om, at BIT har været omfattet af KK's risikostyringsprojekt, således at der er foretaget en risikovurdering samt konsekvensanalyse af udvalgte områder i BIT. Yderligere har BIT gennemført en uafhængig risikovurdering af deres centrale netværksudstyr.

Hvad angår leverandørstyring, er det oplyst, at BIT anvender de rammeaftaler, som kommunen har implementeret. Alle BIT's kontrakter meldes ind i det kontraktmanagement spor, som er etableret af KS. Yderligere er vi informeret om, at kontaktmanagement er placeret hos faste medarbejdere i BIT, som periodisk følger op på de indgåede aftaler.

Det er oplyst, at BIT's AD er baseret på UNI-Login oplysninger fra Styrelsen for It og Læring (STIL). Endvidere har STIL aldrig har haft en implementeret password-politik på UNI-Login. Brugerne (elever og pædagogiske medarbejdere) skal selv stå for at skifte deres password med jævne mellemrum. Det ændrede password bliver synkroniseret til BIT's AD.

Endvidere har vi fået oplyst, at det i forbindelse med det nye UNI-Login fra STIL er besluttet, at både elever og pædagogiske medarbejdere skal anvende BIT's AD til login til AULA, læringsplatforme, digitale læremidler mv. således, at med denne beslutning skulle der implementeres passwordpolitikker baseret på KK's krav.

I forbindelse med revisionen af 2020 har vi foretaget en gennemgang af den faktisk implementerede sikkerhed hos BIT i form af konkrete test af adgange samt den opsatte sikkerhed. Det er her konstateret, at der ikke opsat tvunget periodisk skift af password for brugerne, som tilgår BIT's AD, baseret på KK's generelle krav til passwordpolitik.
Det er dog oplyst, at der foreligger en handleplan til at få bragt området på plads, således at det lever op til de generelle retningslinjer i KK. Det er endvidere oplyst, at BIT ikke har implementeret tvunget periodisk skift af password endnu grundet COVID19. Efter det oplyste ligger der en handleplan klar til godkendelse i BUF med henblik på implementering, når arbejdssituationen tillader det.

Leverandørstyring

Historisk har revisionen modtaget relevante revisionserklæringer medio revisionsåret, og der har været en lang reaktionstid på opfølgning og udbedring af rapporterede svagheder i erklæringerne.

Vi har i forbindelse med revisionen af 2020 fulgt op på processen vedrørende leverandørstyring, herunder hvorledes det sikres, at de indgåede aftaler overholdes, processen for anmodning om systemrevisionserklæringer fra KMD samt proceduren for opfølgning af eventuelle observationer i systemrevisionserklæringer.

Vi har i forbindelse med vores gennemgang fået oplyst, at der afholdes periodiske leverandørstyrgruppemøder med KMD, hvor de mere overordnede aftaler, herunder status på systemrevisionserklæringer, drøftes og gennemgås. Det er oplyst, at der i forbindelse med disse møder er indgået aftale med KMD om, at systemrevisionserklæringer på Kvantum fremadrettet skal foreligge senest den 1. marts.

Yderligere afholdes månedlige driftsmøder, hvor KMD's SLA-rapporter gennemgås, og hver 14. dag afholdes vedligeholdelsesmøder, hvor blandt andet det daglige vedligehold, samarbejdsrelationer mv. drøftes og gennemgås.

Vi har i forbindelse med vores gennemgang konstateret, at der i samarbejde med KMD er igangsat forbedrende tiltag med henblik på at lukke de afvigelser, som KMD's revisor har konstateret i forhold til Kvantum. Vi har endvidere modtaget en vurderings af KMD's opfølgning på åbne observationer fra KMD's revisor, hvori det er oplyst, at 5 ud af 9 observerede afvigelser er lukket i pågældende revisionsperiode. Det er oplyst, at der fortsat pågår arbejde for at lukke de resterende afvigelser.

Vi vil følge op på disse, når den endelige systemrevisionserklæring for 2020 er modtaget.

SharePoint Online (SPO)

Datatilsynet har den 7. januar 2019 rettet henvendelse til Københavns Kommune, idet tilsynet via et anonymt tip den 12. december 2018 er blevet orienteret om, at Københavns Kommune benytter cloudplatformen SharePoint til deling af filer, hvori personoplysninger, herunder fortrolige personoplysninger, om kommunens medarbejdere indgår, og at der ved disse delinger videregives fortrolige personoplysninger om kommunens medarbejdere til uvedkommende.

Der er fra Datatilsynet truffet følgende afgørelse:
Efter en gennemgang af sagen finder Datatilsynet grundlag for at udtale alvorlig kritik af, at Københavns Kommunes behandling af personoplysninger ikke er sket i overensstemmelse med databeskyttelsesforordningens artikel 32.

SPO er en webbaseret løsning, som kan bruges til vidensdeling og dokumentstyring. SPO benyttes oftest igennem en browser og fungerer på mange måder som en traditionel hjemmeside. Afdelinger, projektgrupper og enkeltpersoner kan lave egne foldere/mapper, som kan ligge under de mere overordnede sites.

SPO er ikke tiltænkt at skulle opbevare data om hverken borgere eller ansatte i længere tid.

Det er i forbindelse med vores møde med KK oplyst, at der er igangsat et forvaltningsfælles oprydningsprojekt, som blandt andet har til formål at få ryddet op i data på fællesdrev, herunder klassificere og ansvarsplacere data samt gennemgå og begrænse adgange til data.

Der er i forbindelse med projektet udarbejdet retningslinjer samt vejledning til opbevaring af filer i SPO, som er sendt ud til de respektive forvaltninger.

Vi har konstateret, at KK i 2020 har arbejdet målrettet med udbedringen af kritikken fra Datatilsynet, hvorfor alle forvaltninger med undtagelse af BUF har indmeldt de nødvendige medlemmer på deres SharePoint-sites.
På baggrund heraf, er der afviklet scripts på hver SharePoint-site, hvor alle unikke rettigheder er blevet fjernet fra eksisterende medlemmer og derefter indlæst indmeldingerne af medlemmer fra hver forvaltning.

Derudover har forvaltningerne gennemgået deres data med fokus på filer, som ikke har været redigeret i mere end 15 måneder via Excel-udtræk med en liste over disse filer, som indeholdt metadata på filerne og på baggrund heraf valgt, hvilke filer der skulle slettes. Derefter har KK anvendt et script eksekveret på SharePoint-sitet til at slette filer, som blev vurderet unødvendige. Denne liste viser således også, hvad der er blevet slettet, og hvad der er beholdt. Efter det oplyste, har nogle forvaltninger valgt at oprette et arkiv for filer ift. efterfølgende dokumentationsbehov.

De bevarede filer på arkiv-sitet har fået frataget samtlige rettigheder samt fået pålagt en karensperiode. Det er endvidere oplyst, at det hos forvaltningerne er O365-koordinatoren, som er en formaliseret rolle med overordnet ansvar for forvaltningens arbejde med O365, som har adgang til arkivfiler, hvorfor øvrige medarbejdere skal henvende sig til denne, hvis de skal bruge en fil – som i givet fald kan overflyttes til sagshåndteringssystemet.
De forskellige karensperioder og slettefrister for arkiverede filer er alle opsat i samarbejde mellem forvaltningerne og KKs DPO.

Vi har konstateret, at BUF er den eneste forvaltning, som ikke er i mål, men at de forventer at være i mål Q1 2021.
Ud fra en risikovurdering har BUF valgt at fokusere på at begrænse rettigheder fremfor filsletning.

Vi vil derfor følge op på dette punkt til næste års revision for at sikre, at BUF er kommet i mål med oprydningsprojektet.

1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2020 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 fem revisionsbemærkninger samt fire revisionsbemærkninger, som vi har kunne lukke. Af de afgivne revisionsbemærkninger kan:

- Ingen revisionsbemærkninger henføres til nye bemærkninger i forbindelse med den udførte IT-revision
- Fem revisionsbemærkninger henføres fra tidligere år til revisionen af årsregnskabet, hvoraf én revisionsbemærkning er blevet nedprioriteret til gul (prioritet 2)
- Fire revisionsbemærkninger fra tidligere år vurderes lukket i forbindelse med den udførte revision.

2.1. Revisionserklæringer

Der forventes modtaget primo 2021 revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser samt en specifik erklæring til Kvantum og en generel erklæring dækkende KMD Opus suiten, herunder KMD Opus Debitor og KMD Opus Løn.

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 bemærkninger (3.4).

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

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

Organisationsområde i KK	ØKF og BIF	**Revisionsområde/ emne**	Generelle IT-kontroller og udvalgte områder til forvaltningsrevision

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.2.1 Styring af brugerrettigheder og systemadgange	**Periodisk revurdering (KMD Opus Debitor, KMD Aktiv og Kvantum)** *Periodisk revurdering -KMD Opus Debitor, KMD Aktiv* Vi har fået oplyst, at der ikke er foretaget en periodisk gennemgang af brugere og tildelte rettigheder i KMD Opus Debitor og KMD Aktiv, ligesom der ikke foretages en vurdering af funktionsadskillelsen i systemerne. Vi er dog bekendte med, at der i forhold til KMD Opus Debitor, er igangsat et projekt med henblik på at vurdere de etablerede roller, herunder roller der kolliderer i kombination. *Periodisk revurdering - Kvantum* Vi har konstateret, at der er udarbejdet og formidlet en forretningsgang samt vejledning vedrørende ledelsestilsyn af brugere og tildelte rettigheder i Kvantum til de respektive forvaltninger. Forretningsgangen foreskriver, at den enkelte forvaltning har ansvaret for gennemførelsen af ledelsestilsynet for egne brugere. Vi har i forbindelse med vores gennemgang konstateret, at	Manglende eller utilstrækkelig kontrol med systemrettigheder og systemadgange til brugere medfører en øget risiko for, at brugeradgange misbruges samt at brugeres rettigheder bliver utidssvarende og ikke afspejler deres arbejdsmæssigt betingede behov.	Vi henstiller, at der foretages en formel vurdering af funktionsadskillelsen i KMD Opus Debitor og KMD Aktiv 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 samme brugere. Vi henstiller, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere i KMD Aktiv, KMD Opus Løn og Kvantum. Vi henstiller, at der i forbindelse med brugeres fratrædelser - såvel medarbejdernes egne opsigelser som afskedigelser - gennemføres en konkret risikovurdering af, hvorledes brugerens rettigheder til systemer, data og net-	2018 2019 2020

	ledelsestilsyn er gennemført for brugere i SAP Kompetencecenteret. Vi har fået oplyst, at der ikke er etableret en central funktion som følger op på, om ledelsestilsyn er gennemført for samtlige forvaltninger. *Fratrædelser (KMD Opus Debitor, KMD Aktiv, Kvantum)* Vi har i forbindelse med vores stikprøvegennemgang af fratrådte brugere konstateret, at en række fratrådte brugere fortsat er aktive i KMD Opus Debitor, KMD Aktiv og Kvantum. **Status 2020** *Periodisk revurdering -KMD Opus Debitor, KMD Aktiv, KMD Opus Løn* Vi har fået oplyst, at der fortsat ikke er foretaget en periodisk revurdering af tildelte rettigheder for brugere oprettet i KMD Aktiv, ligesom der ikke er foretaget en vurdering af funktionsadskillelsen i systemet. For så vidt angår KMD Opus Debitor har vi fået oplyst, at autorisationsprojektet fortsat er igangværende, og at deadline for projektet er sat til 31/3-2021. Derudover er der ikke etableret en procedure for periodisk gennemgang af tildelte rettigheder til brugere i KMD Opus Løn, ligesom den månedlige funktionsadskillelseskontrol vedrørende indberetninger ikke er foretaget konsistent i revisionsperioden. *Periodisk revurdering - Kvantum* Vi har fået oplyst, at forholdet fortsat er uændret. Vi har endvidere fået oplyst, at der er igangsat et projekt med henblik på at implementere en centraliseret løsning for den periodiske revurdering af brugere og tildelte rettigheder på tværs af systemer og forvaltninger. *Fratrædelser (KMD Aktiv)*		værk skal håndteres, og at rettighederne fratages brugeren på baggrund heraf. Vi henstiller, at brugeradministrationsproceduren følges, således at tildeling af rettigheder til brugere sker på baggrund af formelle og dokumenterede autorisationer.	

	I forbindelse med vores stikprøvegennemgang af fratrædelser, har vi konstateret 2 brugere som fortsat er aktive i KMD Aktiv efter deres fratrædelse. *Oprettelser (Kvantum)* I forbindelse med vores stikprøvegennemgang af tildelte udvidede rettigheder har vi konstateret, at 1 af vores stikprøver ikke er udført på baggrund af en formel oprettelsesanmodning.			

Organisationsområde i KK	ØKF	**Revisionsområde/ emne**	Generelle IT-kontroller og udvalgte områder til forvaltningsrevision

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.2.2 Revisionserklæringer	Københavns Kommune har indgået aftale med KMD omkring drift af Kvantum, KMD Aktiv, KMD Opus Debitor, KMD Opus Løn og tilhørende platforme. Vi har konstateret, at Københavns Kommune har anmodet deres leverandør om årligt at afgive en revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser samt en årlig specifik erklæring vedrørende Kvantum og KMD Aktiv. Det er oplyst, at det er aftalt med KMD, at systemrevisionserklæring for Kvantum skal foreligge senest den 1. marts. Vi har dog fået oplyst, at der ikke er afgivet en specifik erklæring for KMD Opus Debitor eller KMD Opus Løn. Der kan således være forhold og risici relateret til blandt andet ændringshåndteringen, som vi er ikke bekendt med. **Status 2020** Vi har konstateret, at der er igangsat en proces til lukning af de oplistede bemærkninger i revisionserklæringerne. Der vil blive fulgt op på forholdene, når erklæringerne for 2020 foreligger. Disse forventes primo 2021.	En manglende eller utilstrækkelig overvågning af underleverandører medfører risiko for, at underleverandører ikke efterlever det forventede IT-sikkerhedsniveau.	Vi henstiller, at der indhentes en specifik revisionserklæring for KMD Opus Debitor og KMD Opus Løn for at opnå en højere grad af sikkerhed. Endvidere vil vi følge op på, at der indhentes relevant revisionserklæring vedr. Kvantum for 2020 til sikring af, at de konstaterede forhold i 2019, er lukket.	2017 2018 2019 2020

Organisationsområde i KK	BUF	Revisionsområde/ emne	BUF IT-drift (BIT)

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.2.3 BUF IT-drift	*BUF IT-drift* Vi har konstateret, at BIT's AD er baseret på UNI-Login oplysninger fra Styrelsen for It og Læring (STIL). Endvidere er det oplyst, at STIL aldrig har haft en implementeret passwordpolitik på UNI-Login. Brugerne (elever og pædagogiske medarbejdere) skal selv stå for at skifte deres password med jævne mellemrum. Det ændrede password bliver synkroniseret til BIT's AD. Endvidere har vi fået oplyst, at der er i forbindelse med, at STIL kommer med et nyt UNI-Login den 18. februar 2020, hvor de ikke længere tilbyder password-synkronisering, har BUF's direktion besluttet, at både elever og pædagogiske medarbejdere fremover skal anvende BIT's AD til login til AULA, læringsplatforme, digitale læremidler mv. således, at man med denne beslutning implementerer BIT også passwordpolitikker baseret på KK's krav. **Status 2020** Vi har konstateret, at der ikke er opsat tvunget periodisk skift af password for brugerne, som tilgår BIT's AD baseret på KK's generelle krav til passwordpolitik. Det er dog oplyst, at der foreligger en handleplan til at få bragt området på plads, således at det lever op til de generelle retningslinjer i KK. Det er endvidere oplyst, at BIT ikke har implementeret tvunget periodisk skift af password endnu grundet COVID19. Efter det oplyste ligger handleplanen klar til godkendelse i BUF. På baggrund heraf opretholdes punktet.	Manglende passwordskift medfører risiko for, at det ønskede IT-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at der arbejdes videre med implementeringen af periodisk passwordskift, således at løsningen bliver underlagt det ønskede IT-sikkerhedsniveau, som er fastlagt af KK.	2019 2020

3.3. Revisionsbemærkninger/observationer fra sidste år, der i forbindelse med IT-revisionen er konstateret lukket

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

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.3.1 Kvantum – Change management - Test	Vi har fået oplyst, at der pr. 1. april er etableret krav til den gennemførte tests omfang samt dokumentation. Vi har i forbindelse med vores stikprøvegennemgang af gennemførte ændringer konstateret, at testdokumentation for 7 ud af 25 ændringer ikke kunne leveres. De 7 ændringer blev idriftsat før den 1. april 2019. Vi nedprioriterer punktet og forventer, at denne kan lukkes i forbindelse med revisionen 2020. **Status 2020** Vi har i forbindelse med vores stikprøvegennemgang af udvalgte ændringer til Kvantum konstateret, at der for samtlige er gennemført en dokumenteret og godkendt test. Punktet lukkes.	Manglende eller utilstrækkelig anvendelse og godkendelse af testplaner og -scenarier i forbindelse med test af ændringer medfører risiko for, at kvaliteten og omfanget af gennemførte test og resultaterne heraf ikke er i overensstemmelse med forventningerne, og dermed at der idriftsættes fejlbehæftede tilretninger.		
3.3.2 IT-risikovurderinger	Vi har konstateret, at risikoappetit og risikohåndteringsplaner er forelagt koncerndirektionen i september 2019. Dog er det konstateret, at der udestår, at forvaltningerne får lukket de af KIT fremsatte henstillinger vedrørende risikovurderingerne for 2018. På baggrund heraf opretholdes punktet. **Status 2020** Vi har fået oplyst, at risikovurderingen i 2019 af kommunens 61 systemer på tværs af forvaltningerne,	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.		

	har resulteret i 146 henstillinger og 332 anbefalinger. På baggrund af direktionsgodkendte handleplaner, er 47 henstillinger og 97 anbefalinger efterlevet pr. august 2020. Vi kan konstatere, at KIT's risikovurderinger laves årligt, og dermed vil der tilkomme nye henstillinger og anbefalinger, som forvaltningerne skal have fokus på at lukke. Endvidere kan vi konstatere, at der pr. august 2020 var 3 systemer hos BUF, som skulle risikovurderes på ny grundet større ændringer. Re-risikovurdering er foretaget og afrapporteret pr. december 2020, hvormed de 3 systemer hos BUF ikke længere udestår. Vi kan dermed konstatere, at KIT's koncept for risikovurderinger er fuldt implementeret. På baggrund heraf lukkes punktet.			
3.3.3 Governance-modellen for anvendelse af SIEM	Det primære formål med at implementere SIEM-løsningen er for at detektere trusler mod kritiske aktiver i tide til at kunne afbøde den skade truslerne kunne forårsage eller ideelt set helt at undgå truslerne. For at opnå dette formål er risikohåndteringsprocessen i de syv forvaltninger afgørende. Ved vores workshop har vi fået oplyst, at kendskabet i forvaltningerne til risikohåndteringsprocessen er begrænset. Vi har endvidere fået oplyst, at forvaltningernes kendskab til ISO 27001, som Københavns Kommune skal følge, ligeledes er begrænset. Vi har endvidere konstateret, at der i forvaltningerne mangler en general forståelse af, hvad SIEM-monitoreringsteamet varetager.	En manglende eller utilstrækkelig governance af SIEM-løsningen medfører risiko for, at det etablerede IT-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.		

	Et af de vigtigste områder i forhold til at forbedre modenheden af informationssikkerhedsniveauet (i dette tilfælde SIEM) er den dokumentation og de retningslinjer, som supporterer SIEM-løsningen. Dokumentation skal være passende, effektivt kommunikeret til relevante parter, have korrekt ejerskab og kunne håndhæves. Dokumentation skal også beskrive sikkerhedsformålet, og hvordan det tilsigtes opnået. Ved vores revision har vi konstateret, at der mangler en general revurdering af dokumentationen og retningslinjerne, som understøtter SIEM-løsningen med det formål at få opbygget den korrekte struktur og få maximeret udbyttet af dokumentationen. **Status 2020** Vi har modtaget den afsluttende rapportering på logopfølgningsprojektet (20. februar 2020). Vi kan konstatere, at 32 ud af 36 systemer nu logges, samt at de resterende 4 har en saglig begrundelse for undtagelse fra logning. Desuden kan vi konstatere, at der er beskrevet standard use-cases, ugentlige rapporter og alarmer samt overgangen til drift, hvor KIT har gennemgået nye logopfølgningsregler med alle forvaltninger. På baggrund heraf har vi stikprøvevist gennemgået use-case-eksempler på KMD Aktiv samt Kvantum for at efterteste, hvorvidt implementeringen heraf er testet og godkendt forud for idriftsættelsen. Dette har ikke givet anledning til bemærkninger. Endvidere har vi stikprøvevist gennemgået eksempler på den gennemførte opfølgning på udløste alarmer, hvilket ikke har givet anledning til bemærkninger.			

	Samtidigt kan vi konstatere, at KIT har implementeret risiko awareness uddannelse for alle stemejere i KK. Det skyldes efter det oplyste, at det derved sikrer en bedre og mere kontinuerlig fokus på risiko og uddannelse end enkeltstående workshops om emnet. Vi kan dermed konstatere, at projektet er afsluttet og fuldt implementeret. På baggrund heraf lukkes punktet.			
3.3.4 Governance-modellen for udvikling og drift af robotter / automatiserede processer	Vi har konstateret, at der ikke foretages en formel revurdering af tildelte rettigheder til UiPath, som benyttes til administration og driftsovervågning af robotterne. Vi har stikprøvevist gennemgået dokumentation for udførte testhandling inden en robot idriftsættes. Vi har konstateret, at testhandlinger ikke formelt dokumenteres. Vi har fået oplyst, at KIT foretager driftsovervågning, men at forvaltningerne er ansvarlige for den forretningsmæssige overvågning af deres robotter. Vi har dog konstateret, at denne ansvarsfordeling ikke er formelt dokumenteret. **Status 2020** Vi har i forbindelse med vores stikprøvegennemgang indhentet og gennemgået robotter, som er implementeret før KIT overtog styringen. Vi har derved testet, at alle idriftsatte robotter, løbende bliver opdateret og i den forbindelse også gennemgår den implementerede governance model. Gennemgangen har ikke givet anledning til bemærkninger. På baggrund heraf lukkes punktet.	En manglende eller utilstrækkelig governance af automatiserede processer medfører risiko for, at det etablerede IT-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.		

3.4. Andre bemærkninger

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

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.4.1 Kvantum – Standardprofiler med udvidede rettigheder	*SAP* og DDIC* Vi har konstateret, at SAP standardbrugerne hos KMD for SAP* og DDIC ikke er blevet låst eller udløbet. **Status 2020** Vi har i forbindelse med opfølgningen på sidste års observation konstateret, at de to brugere fortsat er aktive, men at de kun kan tilgås via secure server hos KMD. Vi har gennemgået loggen over anvendelsen og kan konstatere, at SAP* ikke har været anvendt i perioden, samt at DDIC har været anvendt i forbindelse med patchning i starten af revisionsperioden. Endvidere har vi konstateret, at der pr. januar måned er lavet aftale med KMD om deaktivering af de to brugere. Samtidigt er der opsat en ny proces for aktivering og anvendelse af de to brugere, hvor der kræves case by case review af anvendelsen. Vi vil efterteste denne proces i forbindelse med næste års revision. Baseret på den fremlagte proces forventer vi at kunne lukke punktet i forbindelse med næste års revision.	Manglende eller utilstrækkelig sikkerhed for SAP-standard super brugere SAP* og DDIC, forøger risikoen for, at disse bruger-ID'er anvendes til at opnå uautoriseret adgang til SAP, da disse bruger-ID'er er oplagte mål for indtrængere.	Vi henstiller, at SAP* og DDIC låses for at reducere risikoen for misbrug.	2018 2019 2020

Organisationsområde i KK	BUF	Revisionsområde/ emne	Generelle IT-kontroller og udvalgte områder til forvaltningsrevision

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.4.2 SharePoint	*SharePoint* Vi har konstateret, at Københavns Kommune primo 2019 har gennemført en risikovurdering samt en konsekvensanalyse af Microsoft SharePoint Online og brugen heraf med henblik på at vurdere, hvorvidt der er behov for at iværksætte yderligere tekniske eller organisatoriske sikringsforanstaltninger for at beskytte personoplysninger og værdidata. I forlængelse af risikovurderingsprojektet er der konstateret områder, hvor forbedrende tiltag er iværksat. Sideløbende med det er der igangsat et forvaltningsfælles oprydningsprojekt, som blandt andet har til formål at vurdere og klassificere data i SPO, vurdere rettighedsstyringen, herunder definere dataejere samt vurdere og gennemgå adgange til data. Det er yderligere oplyst, at der ikke er fastlagt endelige datoer for, hvornår projektet forventes afsluttet. Der er fra Datatilsynet truffet afgørelse i sagen, som retter følgende afgørelse: Efter en gennemgang af sagen finder Datatilsynet grundlag for at udtale alvorlig kritik af, at Københavns Kommunes behandling af personoplysninger ikke er sket i overensstemmelse med databeskyttelsesforordningens artikel 32. **Status 2020** Vi har konstateret, at alle forvaltninger med undtagelse af BUF har færdiggjort oprydningsprojektet på SharePoint løsningen. Vi har dog konstateret, at BUF er den eneste forvaltning, som ikke har færdiggjort oprydningsprojektet,	En manglende eller utilstrækkelig governance af SPO-løsningen medfører risiko for, at det ønskede IT-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at oprydningsprojektet forsættes og gennemføres hos BUF efter planen.	2019 2020

Ref.	Observation	Risikobeskri-velse	Anbefaling	Risiko og væsentlig-hed
	men at de efter det oplyste forventer at være i mål Q1 2021. Det er dog forventningen, at BUF vil være færdige med rettighedsoprydning med udgangen af november 2020. Ud fra en risikovurdering har BUF valgt at fokusere på at begrænse rettigheder fremfor filsletning. På baggrund af, at der alene mangler færdiggørelse af oprydningsprojektet i BUF nedprioriteres punktet og vi forventer, at denne kan lukkes i forbindelse med revisionen 2021.			

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

Vi har konstateret følgende væsentlige områder til forbedring:

- Der bør ryddes op i Kvantums SAP-system, og standardbrugere og privilegerede rettigheder bør nedbringes og begrænses til medarbejdere med et arbejdsbetinget behov
- Brugeradministrationsprocessen bør generelt styrkes og formaliseres yderligere, herunder kontroller for tildeling af adgange og rettigheder, lukning af adgange samt periodisk revurdering af tildelte rettigheder.

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 Thomas Kühn på telefon 3093 6227.

København, den 18. februar 2021

Deloitte
Statsautoriseret Revisionspartnerselskab

Lars Kronow
statsautoriseret revisor

Thomas Kühn
partner

NIEG/as
T:\Afd1180\Københavns Kommune\2021\Københavns Kommune – GIK rapport 2020 END 180221.docx