Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr.: 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36 10 20 30
www.deloitte.dk

København Kommune
Økonomiforvaltningen
København Rådhus
1599 København V

Revisionsrapport – Revision af generelle IT-kontroller 2022

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2022 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.

Det har ikke været muligt at foretage en vurdering af de interne kontroller, som KMD og KOMBIT varetager på vegne af Københavns Kommune, idet de rekvirerede systemrevisionserklæringer først forventes modtaget i Q1 23 og senest 31. marts 2023. Deloitte vil foretage gennemgang af systemrevisionserklæringerne, når disse foreligger.

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 KY, 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 efterfølgende 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 KY.

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 og KMD Opus Løn samt tilhørende platforme. Yderligere har kommunen aftale med Kombit omkring drift af KY-applikationen.

Der modtages årligt en revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser samt en årlig specifik erklæring for Kvantum, KMD Opus Debitor og KMD Opus Løn. For så vidt angår systemet KY, har Københavns Kommune for indeværende revisionsperiode ligeledes rekvireret en specifik systemrevisionserklæring til verifikation af, at de outsourcede kontroller gennemføres betryggende.

Forvaltningsrevision
Forvaltningsrevisionen har omfattet nedennævnte områder:

- Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System)
- Risikovurderinger for alle væsentlige it-aktiver, herunder systemer og processer
- Leverandørstyring (opfølgning på tidligere observationer)
- BUF IT-drift (opfølgning på tidligere observationer).

1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2022 og ved interviews af relevant personale hos Københavns Kommune samt ved observationer og stikprøvevis gennemgang af udleveret materiale.

2. Ledelsesresumé og konklusion

Truslerne på informationssikkerhedsområdet er konstant stigende og antallet af virksomheder og myndigheder, der har været udsat for alvorlige hændelser som følge af cyberangreb eller andre alvorlige IT-sikkerhedsmæssige hændelser er tilsvarende stigende. KK har derfor behov for løbende at vurdere tilstrækkeligheden af de etablerede sikringsforanstaltninger, herunder sikre, at der er et ledelsessystem med tilstrækkelige kompetencer, ressourcer og uafhængighed på informationssikkerhedsområdet.

Som omtalt i revisionsberetningen for 2021 har vi haft en indledende drøftelse med Koncern IT (KIT) vedrørende den nuværende organisering på informationssikkerhedsområdet samt planer for styrkelse af informationssikkerheden og det ledelsessystem, der understøtter dette.

I forlængelse heraf er der nedsat et projekt "Et styrket ISMS" og tilknyttet en styregruppe.

Vi har noteret os, at status på dette arbejde i oktober 2022 er følgende:

- **Styrkelse af ledelsessystemet for informationssikkerhed baseret på ISO 27001 (ISMS)**
  Vi har fået oplyst, at der vil blive udarbejdet en analyse, der har til formål at identificere hvilke elementer, der fungerer tilfredsstillende i forhold til et velfungerende ISMS samt identificerer behov for nødvendige tiltag der sikrer et velfungerende ISMS, der er passende for en organisation og et IT-miljø af KKs størrelse og kompleksitet.

  Vi har noteret os, at GAP-analysen vil være grundlaget for at styregruppen kan beslutte videre arbejde med et styrket ISMS i Københavns Kommune.

  Det videre arbejde forventes blandt andet at omfatte initiativer i forhold til løbende rapportering på informationssikkerhedsområdet samt en dokumenteret vurdering af, hvilke af ISO 27001's foreslåede kontroller, der er relevante at implementere (dokumenteret i et SoA-dokument). Sammen med risikovurderingen vil SoA ("Statement of Applicability")-dokumentet danne grundlag for at planlægge, udføre, kontrollere og kontinuerligt forbedre informationssikkerheden.

- **Vurdering af, hvorledes styring af informationssikkerhed mest hensigtsmæssigt organiseres og styrkes**
  Vi noterede os, i forbindelse med revisionen i 2021, at der var behov for at sikre passende ressourcer med de nødvendige kompetencer og den nødvendige uafhængighed til at styrke tilsynet med informationssikkerhed i KK. Der er fortsat behov for at etablere en effektiv tilsynsfunktion.

Et element i et velfungerende ISMS er effektiv planlægning baseret på risikovurderinger for alle væsentlige IT-aktiver, herunder systemer og processer. Vi har i forbindelse med revisionen indhentet og gennemgået udvalgte risikovurderinger, ligesom vi har drøftet processen for udarbejdelse af risikovurderinger generelt.

Vi har noteret os, at risikovurderinger af systemer ikke foretages for alle systemer, men kun de systemer der enten har været i drift i minimum fire år, eller hvor forvaltningen er usikker på om informationssikkerhedsniveauet er tilstrækkeligt, samt for systemer der anvendes tværgående i KK's forvaltninger.

De nuværende risikovurderinger af systemer bør styrkes, således at det sikres, at alle relevante systemer bliver omfattet og med afsæt i opdaterede trusselsvurderinger, herunder at der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt.

Vi har noteret os, at KK arbejder på at ændre risikovurderingsmetoden til at være mere baseret på en egentlig vurdering af risici på baggrund af opdaterede trusselsvurderinger. På tidspunktet for vores revision var denne tilgang dog endnu ikke implementeret i væsentligt omfang og omfattede kun meget få trusselsscenarier.

Leverandørstyring

Vi har i forbindelse med revisionen af 2021 revideret processen vedrørende leverandørstyring, særligt processen for IT-anskaffelser samt ansvarsfordeling og retningslinjer for leverandørstyring, herunder processer og retningslinjer for løbende monitorering af leverandører.

Vi har fået oplyst, at Københavns Kommune de senere år har indført en ny Governance-model for IT-anskaffelser. Vi har i forbindelse med vores revision konstateret, at IT-anskaffelser følger en styret proces, der omfatter flere faser til sikring af, at der bliver foretaget de nødvendige behovsanalyser, risiko- og sikkerhedsvurderinger samt forligger de fornødne godkendelser før anskaffelse af nye IT-systemer og endelig idriftsættelse heraf.

Vi har ved vores revision dog konstateret, at ældre systemer ikke følger den nye Governance-model for IT-anskaffelser.

Vi har fået oplyst, at KIT initierede en intern analyse på tværs af alle forvaltninger i Københavns Kommune i 2020. Formålet var at belyse systemejerrollen i Københavns Kommune. Analysen mundede ud i 8 hovedobservationer, hvor særligt én har haft betydning for vores revision, herunder H7 - *utilstrækkelig styring af kontrakter og leverandører på det enkelte IT-system*.

Vi har i forbindelse med vores revision konstateret, at der på baggrund af den interne systemejeranalyse er udarbejdet handleplan med forbedrende tiltag, der har til formål at professionalisere systemejerrollen i Københavns Kommune, herunder processen for leverandørstyring.

Vi har i forbindelse med revisionen af 2021 konstateret, at Københavns Kommune har processer til sikring af, at roller og systemejerskab er klart defineret og placeret, men at der ikke foreligger klare retningslinjer for leverandørstyring, som er gældende på tværs af forvaltningerne. Processen er forankret i de enkelte forvaltninger, hvilket gør, at monitorering og opfølgning ikke sker i tilstrækkelig grad.

Vi har i forbindelse med revisionen af 2022 fulgt op på udmøntningen af systemejeranalysen. Vi har konstateret, at Københavns Kommune i regi af arbejder på systemejerområdet har igangsat forbedrende tiltag i form af implementering af værktøjer og metoder til udførelse af konkrete systemejeropgaver, herunder leverandørstyring.

Yderligere er der i revisionsperioden gennemført en foranalyse vedrørende IT-kontraktstyring med henblik på at forbedre kontraktstyringen på tværs af forvaltningerne.

Det er oplyst, at foranalysen har givet anledning til en række anbefalinger, som kommunen har taget til efterretning og vil med DCK som styregruppe igangsætte arbejder med henblik på at implementere forbedrende tiltag.

Der henvises til afsnit 3 og 4 for uddybning af ovenstående og andre relevante forhold.

3. Observationer, risikovurdering og anbefaling

Observationer opdeles i henholdsvis:

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

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

Organisationsområde	ØKF	Revisionsområde/emne	Ibrugtagningstilladelser

Reference	Observationer og risici	Revisionsbemærkning	Omtalt år
3.1.1 Ibrugtagning af IT-systemer	*Ibrugtagningstilladelse* Den nye borgerserviceplatform i Kultur- og Fritidsforvaltningen (KFF), der anvendes til at udstede pas og kørekort, blev taget i brug d. 27. juli 2022 uden en ibrugtagningstilladelse. KFF og KIT samarbejdede sideløbende om at bringe de tekniske og sikkerhedsmæssige udfordringer i orden. KIT orienterede i juli 2022 KFF om, at en ibrugtagningstilladelse ikke ville kunne gives inden borgerplatformen skulle idriftsættes den 27. juli 2022, da der ikke forelå en fyldestgørende handleplan for at håndtere de tekniske og sikkerhedsmæssige udeståender. Den 2. september forelå en ibrugtagningstilladelse, som indeholdt en liste over 29 tekniske udeståender. KIT kan på det tidspunkt ikke udstede en officiel ibrugtagningstilladelse til systemet. KFF har efterfølgende udarbejdet en handleplan, der imødegår problemstillingerne, og Koncern IT har udstedt en betinget ibrugtagningstilladelse med handleplan d. 26. september 2022.	Af Forretningscirkulæret for IT-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt IT-system skal sikkerhedsvurderes inden det idriftsættes. En sikkerhedsvurdering tager stilling til, at alle krav til informationssikkerhed og databeskyttelse er opfyldt. På baggrund af sikkerhedsvurderingen udstedes en ibrugtagningstilladelse. IT-systemer skal have en ibrugtagningstilladelse inden de idriftsættes. Da KIT meddelte KFF, at en ibrugtagningstilladelse ikke ville kunne udstedes forud for idriftsættelsen, burde sagen derfor have været behandlet som uoverensstemmelse. Dette indebærer en eskalering til hhv. DCK og ITK, hvor der skal opnås enighed, hvis sagen ikke skal eskaleres yderligere til de relevante administrerende direktører, borgmestre og ultimativt til ØU. Det er forbundet med stor risiko for kommunen at idriftsætte et IT-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse. Det henstilles, at forvaltningerne følger anskaffelsesprocessen, og Koncern IT følger eskalationsprocessen, hvis en tilsvarende sag opstår. Det henstilles samtidig, at KIT undersøger, om der er flere IT-systemer der er idriftsat uden at der foreligger en ibrugtagningstilladelse.	2022

Organisationsområde	ØKF	Revisionsområde/emne	ISMS

Reference	Observationer og risici	Revisionsbemærkning	Omtalt år
3.1.2 Organisering af informationssikkerhed og styrkelse af det ISMS	*Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System).* På baggrund af de konstant stigende trusler på informationssikkerhedsområdet er der behov for løbende at vurdere tilstrækkeligheden af de etablerede sikringsforanstaltninger, herunder sikre, at der er et ledelsessystem med tilstrækkelige kompetencer, ressourcer og uafhængighed på informationssikkerhedsområdet. KK har erkendt behovet herfor og har nedsat et projekt med tilknyttet styregruppe, der har til formål at sikre et styrket ISMS. Det er vores forståelse, at projektet vil arbejde med styrkelse af ledelsessystemet for informationssikkerhed baseret på ISO 27001 (ISMS). Dette omfatter blandt andet forbedring af risikovurderinger, implementering af relevante sikringsforanstaltninger og rapportering på informationssikkerhedsområdet. Yderligere vil organisering af informationssikkerhedsområdet ligeledes blive vurderet, herunder sikre passende ressourcer med de nødvendige kompetencer og den nødvendige uafhængighed til at overvåge informationssikkerheden.	Vi henstiller, at arbejdet med at styrke informationssikkerheden prioriteres højt, herunder at der: • Foretages en GAP-analyse af det nuværende ISMS med henblik på at identificere mere specifikt, hvilke områder der skal styrkes • Med afsæt heri vurderes, hvorledes organiseringen af informationssikkerhedsområdet bør være, således at dette sikrer tilstrækkelige kompetencer og uafhængighed • Der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt.	2022

Organisationsområde	ØKF	Revisionsområde/emne	Risikovurderinger

Reference	Observationer og risici	Revisionsbemærkning	Omtalt år
3.1.3 Risikovurderinger	Vi har i forbindelse med revisionen indhentet og gennemgået udvalgte risikovurderinger, ligesom vi har drøftet processen for udarbejdelse af risikovurderinger generelt. Vi har noteret os, at risikovurderinger af systemer ikke foretages for alle systemer, men kun de systemer der enten har været i drift i minimum fire år, eller hvor forvaltningen er usikker på om informationssikkerhedsniveauet er tilstrækkeligt, samt for systemer der anvendes tværgående i KK's forvaltninger. I forhold til de foretagne risikovurderinger har vi noteret os, at disse er baseret på en liste af "standard" kontrolområder. Der ligger ikke et egentlig opdateret trusselskatalog til grund for disse risikovurderinger. Ligeledes kan vi ikke, på baggrund af den foreliggende dokumentation, se, at der er konsekvent, foretages en dokumenteret vurdering af, hvorvidt de mitigerende sikringstiltag og kontroller faktisk fungerer hensigtsmæssigt. Vi har noteret os, at KK arbejder på at ændre risikovurderingsmetoden til at være mere baseret på en egentlig vurdering af risici på baggrund af opdaterede trusselsvurderinger. På tidspunktet for vores revision var denne tilgang dog endnu ikke implementeret i væsentligt omfang og omfattede kun meget få trusselsscenarier.	Vi henstiller, at: • De nuværende risikovurderinger af systemer styrkes, således at det sikres, at alle relevante systemer bliver omfattet og med afsæt i opdaterede trusselsvurderinger • Der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt	2022

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

Organisationsområde	Økonomiforvaltningen	Revisionsområde/emne	Generelle IT-kontroller og udvalgte områder til forvaltningsrevision

Reference	Observationer og risici	Revisionsbemærkning	Omtalt år
3.2.1 Outsourcing-leverandørstyring	*Outsourcing- anskaffelsesprocedure og retningslinjer for leverandørstyring* Manglende eller utilstrækkelig styring og monitorering af leverandører medfører risiko for, at de leverede ydelser ikke dækker forretningsmæssige behov, samt at leverandører ikke efterlever det forventede IT-sikkerhedsniveau. Vi har konstateret, at IT-anskaffelser og kontraktindgåelser for ældre systemer ikke følger Københavns Kommunes Governance-model herfor. Yderligere har vi konstateret, at der ikke foreligger klare retningslinjer for leverandørstyring, som er gældende på tværs af alle forvaltninger. Processen er forankret i de enkelte forvaltninger, hvilket gør, at monitorering og opfølgning ikke sker i tilstrækkelig grad. **Status 2022** Vi har fået oplyst, at Københavns Kommune med DCK som styregruppe har igangsat forbedrende tiltag i form af implementering af værktøjer og metoder med henblik på at konkretisere og operationalisere systemejerrollen, herunder i forhold til leverandørstyring. Ligeledes igangsættes arbejder med henblik på at forbedre IT-kontraktstyringen på tværs af forvaltningerne. Punket opretholdes og forventes lukket ved revisionen af 2023.	Vi henstiller, at leverandørkontrakter undergår Københavns Kommunes Governance-model ved genforhandling. Derudover henstiller vi, at der etableres fælles administrative forretningsgange for opfølgning.	2021 2022

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

Reference	Observationer og risici	Revisionsbemærkning	Omtalt år
3.2.2 BUF IT-drift	*BUF IT-drift* Vi har konstateret, at der ikke er opsat tvunget periodisk skift af password for brugere, som tilgår BIT's AD, baseret på Københavns Kommunes generelle krav til passwordpolitik. Vi er oplyst om, at denne forventes implementeret i forbindelse med implementeringen af den nye nationale standard NSIS, hvor BUF IT-drift er en del af NSIS-projektet. **Status 2022** Vi har fået oplyst, at forholdet er uændret. NSIS-løsningen forventes implementeret primo 2023. Punktet opretholdes og forventes lukket ved revisionen af 2023.	Vi henstiller, at der arbejdes videre med implementeringen af periodisk passwordskift, således at løsningen bliver underlagt det ønskede IT-sikkerhedsniveau, som er fastlagt af Københavns Kommune.	2019 2020 2021 2022

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

I 2022 er der lukket en kritisk bemærkning og en væsentlig observation:

- **Styring af roller og rettigheder – Kvantum**

Vi har fået oplyst, at alle brugere og tildelte roller er gennemgået og vurderet i forbindelse med det nye autorisationskoncept, som er kørt i perioden fra ultimo december 2021 til og med juni 2022.

Yderligere er det oplyst, at ledelsestilsynet i Kvantum fremadrettet forventes gennemført via en centraliseret løsning med henblik på at sikre, at samtlige brugere på tværs af forvaltningerne omfattes af ledelsestilsynet.
Punktet lukkes.

- **Revisorerklæringer**

Vi har konstateret, at Københavns Kommune årligt rekvirerer systemrevisionserklæringer for Kvantum, Opus Løn og Opus Debitor til verifikation af, at de outsourcede kontroller gennemføres betryggende.
Punktet lukkes.

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 Thomas Kühn på telefon 3093 6227.

København, den 9. december 2022

Deloitte
Statsautoriseret Revisionspartnerselskab

Jakob B. Ditlevsen
statsautoriseret revisor

Thomas Kühn
statsautoriseret revisor

TK/as
T:\Afd1180\Københavns Kommune\2022\Københavns Kommune – GIK rapport 2022 END 091222.docx