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

Telefon 36 10 20 30
www.deloitte.dk

Københavns Kommune
Økonomiforvaltningen
Att.: Adm. direktør Søren Hartmann Hede
Københavns Rådhus
1599 København V

# Revisionsrapport – Revision af generelle IT-kontroller 2021

## Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2021 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 varetager på vegne af Københavns Kommune, idet de rekvirerede systemrevisionserklæringer først forventes modtaget i Q1 22 og senest 31. marts 2022. 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 KMD Aktiv, samt om kontrollerne har fungeret i hele revisionsperioden.

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

Deloitte Touche Tohmatsu Limited
Deloitte er en betegnelse for et eller flere af Deloitte Touche Tohmatsu Limiteds ("DTTL") medlemsfirmaer, dets netværk af medlemsfirmaer og deres tilknyttede virksomheder (der samlet betegnes "Deloitte-organisationen"). DTTL (der også omtales som "Deloitte Global") og alle dets medlemsfirmaer og tilknyttede virksomheder udgør selvstændige og uafhængige juridiske enheder, som ikke kan forpligte hinanden over for tredjemand. DTTL og de enkelte DTTL-medlemsfirmaer og tilknyttede virksomheder er kun ansvarlige for egne handlinger og/eller udeladelser. DTTL leverer ikke ydelser til kunder. Vi henviser til www.deloitte.com/about for nærmere oplysninger.

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 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 og KMD Aktiv. For så vidt angår systemerne KMD Opus Debitor og KMD Opus Løn, har Københavns Kommune for indeværende revisionsperiode rekvireret specifikke systemrevisionserklæringer til verifikation af, at de outsourcede kontroller gennemføres betryggende.

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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

- BUF IT-drift opfølgning af observationer fra 2020-revisionen
- Leverandørstyring.

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

**BUF IT-drift**

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, hvoraf 21 er udkørende teknikere, som blandt andet varetager driftssupport.

Yderligere er det oplyst, at BIT på lige fod med de øvrige forvaltninger er underlagt Københavns Kommunes 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.

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 passwords 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 der med denne beslutning skal implementeres passwordpolitikker baseret på Københavns Kommunes krav.

I forbindelse med revisionen af 2020 har vi foretaget en gennemgang af den faktisk implementerede sikkerhed hos BIT i form af konkrete tests af adgange samt den opsatte sikkerhed. Det er her konstateret, at der ikke er opsat tvunget periodisk skift af password for brugerne, som tilgår BIT's AD, baseret på Københavns Kommunes generelle krav til passwordpolitik.

Vi har i indeværende revisionsperiode fulgt op på, hvorvidt observation vedrørende periodisk passwordskift er udbedret. Vi er oplyst om, at BUF IT-drift ved revisionstidspunktet endnu ikke har implementeret periodisk password skift. Det er oplyst, at denne forventes implementeret i forbindelse med implementeringen af den nye nationale standard NSIS, hvor BUF IT-drift er en del af NSIS-projektet.

**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.

I forbindelse med vores revision i 2020 fik vi 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.

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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 vurdering af KMD's opfølgning på åbne observationer fra KMD's revisor, hvori det er oplyst, at der er 5 åbne afvigelser i pågældende revisionsperiode.

Vi vil følge op på disse, når den endelige systemrevisionserklæring for 2021 er modtaget.

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 vil følge op på udmøntningen af systemejeranalysen ved revisionen for 2022.

**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.

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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 Københavns Kommune blevet 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.

I forbindelse med revisionen af 2020 var det konstateret, at samtlige forvaltninger var i mål med oprydningsprojektet med undtagelse af BUF. Vi har i indeværende revisionsperiode fulgt op på status for oprydningsprojektet hos BUF.

Vi har fået oplyst, at BUF i 2021 fortsat har arbejdet målrettet med oprydningsprojektet og i den forbindelse har gennemgået og slettet et større antal filer og mapper fra BUF's SharePoint site. Pr. april 2021 er oprydningsprojektet afsluttet hos BUF og en handleplan, med henblik på en kontinuerlig opretholdelse af compliance i SharePoint, er udarbejdet.

Desuden har vi konstateret, at der pr. uge 42 er implementeret halvårlige ledelsestilsyn på SPO som igangsættes automatisk og omfatter alle siteejere og dataejere.

Vi kan dermed konstatere, at projektet er afsluttet og vedvarende fokus på compliance i SharePoint er opretholdt.

**Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System)**

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.

Vi har haft en indledende drøftelse med KIT vedrørende den nuværende organisering på informationssikkerhedsområdet samt planer for styrkelse af informationssikkerheden og det ledelsessystem, der understøtter dette.

Således har vi noteret os, at KIT vurderer mulige indsatser på informationssikkerhedsområdet. Dette omfatter blandt andet vurdering inden for følgende hovedområder:

- **Styrkelse af ledelsessystemet for informationssikkerhed baseret ISO 27001 (ISMS).** Dette 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.** Dette er tænkt at omfatte en vurdering og præcisering af roller og ansvar for informationssikkerhed på tværs af KIT og forvaltningerne. Yderligere vurderes den organisatoriske

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

placering og eventuelt behov for styrelse af det nuværende tilsyn på informationssikkerhedsområdet med henblik på at sikre de nødvendige kompetencer og uafhængighed på området.

Det er aftalt, at KIT arbejder videre med ovenstående initiativer m.fl., som vil blive indarbejdet i mere detaljerede planer med henblik på implementering i løbet af 2022. Vi vil følge planerne for styrkelse af dette i løbet af 2022 samt teste implementeringen heraf.

### 1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2021 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 åbne bemærkninger og observationer (hvoraf den ene lukkes pr. 1. april 2021) samt tre bemærkninger og observationer, som vi har kunnet lukke. Af de afgivne bemærkninger og observationer kan:

- En observation henføres til nye bemærkninger/observationer i forbindelse med den udførte IT-revision
- To bemærkninger og to observationer henføres fra tidligere år til revisionen af årsregnskabet, hvoraf én bemærkning er blevet nedprioriteret til gul (prioritet 2) og én bemærkning lukkes i april 2021.
- En bemærkning og to observationer vurderes lukket i forbindelse med den udførte revision.

### 2.1. Revisionserklæringer

Der forventes modtaget primo 2022 revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser samt en specifik erklæring til Kvantum, KMD Aktiv og KMD Opus suiten, herunder KMD Opus Debitor og KMD Opus Løn.

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

## 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)

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

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

| **Ref.** | **Observation** | **Risikobeskrivelse** | **Anbefaling** | **Risiko og væsentlighed** |
|---|---|---|---|---|
| 3.1.2 Outsourcing-leverandørstyring | *Outsourcing- anskaffelsesprocedure og retningslinjer for leverandørstyring*<br><br>Vi har konstateret, at IT-anskaffelser og kontraktindgåelser for ældre systemer ikke følger Københavns Kommunes Governance-model herfor.<br><br>Yderligere har vi konstateret, at der ikke foreligger klare retningslinjer for leverandørstyring, som er gældende på tværs af alle forvaltninger.<br><br>Processen er forankret i de enkelte forvaltninger, hvilket gør, at monitorering og opfølgning ikke sker i tilstrækkelig grad. | 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 henstiller, at leverandørkontrakter undergår Københavns Kommunes Governance-model ved genforhandling.<br><br>Derudover henstiller vi, at der etableres fælles administrative forretningsgange for opfølgning og monitorering af leverandørydelser. | 2021 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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

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

| **Ref.** | **Observation** | **Risikobeskrivelse** | **Anbefaling** | **Risiko og væsentlighed** |
|---|---|---|---|---|
| 3.2.1 Styring af roller og rettigheder – Kvantum | *Periodisk revurdering - Kvantum*<br><br>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.<br><br>Vi har i forbindelse med vores gennemgang konstateret, at ledelsestilsyn er gennemført for brugere i SAP Kompetencecenteret.<br><br>Vi har fået oplyst, at der ikke er etableret en central funktion som følger op på, om ledelsestilsyn er gennemført for samtlige forvaltninger.<br><br>**Status 2021**<br><br>Vi har konstateret, at forholdet fortsat er uændret, og der således ikke er implementeret en centraliseret løsning mhp. at sikre, at ledelsestilsyn udføres på tværs af forvaltningerne. Vi har dog fået oplyst, at forholdet forventes udbedret i 2022 i forlængelse af nye, smallere roller til Kvantum, der samtidigt udføres ledelsestilsyn i forvaltningerne og centralt ledelsestilsyn, | 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 periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere i Kvantum. | 2018<br>2019<br>2020<br>2021 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

| 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 | København Kommune har indgået aftale med KMD omkring drift af Kvantum, KMD Aktiv, KMD Opus Debitor, KMD Opus Løn og tilhørende platforme.<br><br>Vi har konstateret, at København 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.<br><br>Det er oplyst, at det er aftalt med KMD, at systemrevisionserklæring for Kvantum skal foreligge senest den 1. marts.<br><br>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.<br><br>**Status 2021**<br><br>Vi har fået oplyst, at København Kommune har rekvireret specifikke systemrevisionserklæringer for Kvantum, KMD Opus Debitor og KMD Opus Løn. Disse forventes modtaget primo 2022.<br><br>Der vil blive fulgt op på forholdende, når erklæringerne foreligger.<br><br>Observationen nedprioriteres og forventes lukket i forbindelse med revisionen af 2022. | 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. | 2017<br><br>2018<br><br>2019<br><br>2020<br><br>2021 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

| 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*<br><br>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 passwords med jævne mellemrum. Det ændrede password bliver synkroniseret til BIT's AD.<br><br>Endvidere har vi fået oplyst, at BUF's direktion (i forbindelse med, at STIL kommer med et nyt UNI-Login den 18. februar 2020, hvor de ikke længere tilbyder password-synkronisering) har 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 også implementerer BIT's passwordpolitikker baseret på KK's krav.<br><br>**Status 2021**<br><br>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 password-politik.<br><br>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.<br><br>Punktet opretholdes. | Manglende password-skift 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 password-skift, således at løsningen bliver underlagt det ønskede IT-sikkerhedsniveau, som er fastlagt af Københavns Kommune. | 2019<br><br>2020<br><br>2021 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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

| Ref. | Observation | Risikobeskrivelse | Anbefaling | Risiko og væsentlighed |
|---|---|---|---|---|
| 3.3.4 Kvantum Standardprofiler med udvidede rettigheder | *SAP* og DDIC*<br><br>Vi har konstateret, at SAP-standardbrugerne hos KMD for SAP* og DDIC er aktive, men at de kun kan tilgås via secure server hos KMD.<br><br>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.<br><br>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.<br><br>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.<br><br>**Status 2021**<br><br>Vi har konstateret, at serviceleverandøren KMD i perioden fra januar 2021 til 1. april 2021 har haft adgang til Kvantum produktionsmiljøet med standardbrugere SAP* og DDIC.<br><br>Vi har i forbindelse med vores IT-revision konstateret, at brugerne låst efter 1. april 2021. | Manglende eller utilstrækkelig sikkerhed for SAP-standard superbrugere 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. | Fra april 2021 er brugerne lukket, og bemærkningen er dermed lukket fra 1. april 2021. | 2018<br><br>2019<br><br>2020<br><br>2021 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

### 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 Styring af brugerrettigheder og systemadgange | *Periodisk revurdering – KMD Opus Debitor, KMD Opus Løn*<br><br>Vi har fået oplyst, at KMD Opus Debitor autorisationsprojektet fortsat er igangværende, og at deadline for projektet er sat til 31/3 2021.<br><br>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.<br><br>**Status 2021**<br><br>Vi har konstateret, at KMD Opus Debitor autorisationsprojektet er afsluttet og brugerroller og brugeradgange samt funktionsadskillelse i KMD Opus Debitor er gennemgået og vurderet. Desuden er procedure for halvårlige ledelsestilsyn implementeret og gennemført.<br><br>For så vidt angår KMD Opus Løn har vi konstateret, at der er implementeret procedure for årlige ledelsestilsyn. Derudover har vi konstateret, at pr. 30. november 2021 er 97 % af brugerne gennemgået, og at en handleplan for de resterende brugere er udarbejdet.<br><br>Observation lukkes. | 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 Opus Løn således, at der på baggrund af en konkret risikovurdering udarbejdes en oversigt over roller/adgangsrettigheder, der ikke bør tildeles samme brugere.<br><br>Vi henstiller, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere i KMD Opus Debitor og KMD Opus Løn. | 2018<br><br>2019<br><br>2020 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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

| Ref. | Observation | Risikobeskrivelse | Anbefaling | Risiko og væsentlighed |
|---|---|---|---|---|
| 3.3.2 SharePoint | *SharePoint*<br><br>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.<br><br>I forlængelse af risikovurderingsprojektet er der konstateret områder, hvor forbedrende tiltag er iværksat.<br><br>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.<br><br>Det er yderligere oplyst, at der ikke er fastlagt endelige datoer for, hvornår projektet forventes afsluttet.<br><br>Der er fra Datatilsynet truffet afgørelse i sagen, som retter følgende afgørelse:<br><br>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. | 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<br><br>2020 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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

| Ref. | Observation | Risikobeskrivelse | Anbefaling | Risiko og væsentlighed |
|---|---|---|---|---|
| | **Status 2021**<br>Vi har konstateret, at alle forvaltninger har færdiggjort oprydningsprojektet på SharePoint-løsningen.<br><br>Yderligere har vi konstateret, at der er implementeret en arbejdsgang med henblik på opretholdelse af kontinuerligt fokus på compliance i SharePoint<br><br>Punktet lukkes. | | | |
| 3.3.3 Styring af roller og rettigheder – KMD Aktiv | *Periodisk revurdering - KMD Aktiv*<br>Vi har fået oplyst, at der ikke er foretaget en periodisk gennemgang af brugere og tildelte rettigheder i KMD Aktiv, ligesom der ikke foretages en vurdering af funktionsadskillelsen i systemet.<br>*Fratrædelser (KMD Aktiv)*<br>I forbindelse med vores stikprøvegennemgang af fratrædelser, har vi konstateret 2 brugere, som fortsat er aktive i KMD Aktiv efter deres fratrædelse.<br>**Status 2021**<br>*Periodisk revurdering - KMD Aktiv*<br>Vi har fået oplyst, at der fortsat ikke er foretaget en periodisk revurdering af tildelte rettigheder for brugere i KMD Aktiv, ligesom der ikke er foretaget en vurdering af funktionsadskillelsen i systemet.<br><br>*Oprettelser (KMD Aktiv)*<br>Vi har konstateret, at 5 af 11 stikprøveudvalgte brugeroprettelser ikke er udført på baggrund af en godkendt anmodning fra | 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. | N/A KMD Aktiv er udfaset pr. oktober 2021 | 2018<br>2019<br>2020<br>2021 |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

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

| Ref. | Observation | Risikobeskrivelse | Anbefaling | Risiko og væsentlighed |
|---|---|---|---|---|
| | nærmeste leder eller autorisationsansvarlig.<br><br>*Fratrædelser (KMD Aktiv)*<br><br>I forbindelse med vores stikprøvegennemgang af fratrædelser har vi konstateret, at en række fratrådte brugere fortsat er aktive i KMD Aktiv efter deres fratrædelse.<br><br>Vi er endvidere bekendte med, at KMD Aktiv systemet er udfaset pr. oktober 2021 | | | |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

## 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.

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

## 4. 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 Thomas Kühn på telefon 3093 6227.

København, den 9. december 2021

**Deloitte**
Statsautoriseret Revisionspartnerselskab

| | |
|---|---|
| Lars Kronow<br>statsautoriseret revisor | Thomas Kühn<br>partner |

Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU

SETU/tnan/as
T:\Afd1180\Københavns Kommune\2021\Københavns Kommune – GIK rapport 2021 END 081221.docx

PENNEO

*Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.*

*"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."*

**Lars Kronow**
**Revisor**
*Serienummer: PID:9208-2002-2-966471939633*
*IP: 83.151.xxx.xxx*
*2021-12-09 11:40:32 UTC*
NEM ID

**Thomas Kühn**
**Revisor**
*Serienummer: CVR:33963556-RID:90946475*
*IP: 93.164.xxx.xxx*
*2021-12-09 12:36:21 UTC*
NEM ID

*Penneo dokumentnøgle: 7XM3L-A4FZE-O7L81-ED5E3-Q3TON-EFGTU*

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

**Sådan kan du sikre, at dokumentet er originalt**
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validate**