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 2019

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2019 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

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

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

Forvaltningsrevision
Forvaltningsrevisionen har omfattet en opfølgning af observationer fra revisionen af 2018 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.

I følgende afsnit har vi beskrevet vores revision og opfølgning af de fire 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 2019 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 2018.

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 2019 har Deloitte fulgt op på tidligere rapporterede observationer vedrørende anvendelse af SIEM og fastholder således anbefaling vedrørende følgende forbedringspunkter:

- Det primære formål med at implementere SIEM-løsningen er at detektere trusler mod kritiske aktiver i tide til at kunne afbøde den skade, som truslerne kunne forårsage, eller ideelt set helt at undgå truslerne. For at opnå dette formål er risikohåndteringsprocessen i de syv forvaltninger afgørende. For at kunne øge kendskabet til den nuværende risikorapporteringsproces og for at fremhæve den positive indvirkning risikorapportering har på alle niveauer, anbefaledes det, at en risiko awarness workshop afholdes for de syv forvaltninger. Workshoppen bør fokusere på følgende områder:

    - Linket mellem en forretningsrisiko og en informationssikkerhedsrisiko
    - Risikoejerskab
    - Risikoidentifikation og rapportering
    - Risk management
    - Risikohåndtering i kontekst med SIEM
    - Praktisk risikodemonstration

- Københavns Kommune er pålagt at følge ISO 27001, som er en industristandard for informationssikkerhedshåndtering. Standarden dikterer, hvordan informationssikkerhed håndteres baseret på risici, og hvordan kontrolforanstaltninger implementeres. Kendskabet i forvaltningerne til processen er afgørende, vi anbefaler derfor, at der afholdes en ISO 27001 awarenes workshop for forvaltninger. Workshoppen bør fokusere på følgende områder

    - Overblik over informationsmanagementsystemet (ISMS)
    - Betydningen af risici i ISMS
    - De obligatoriske klausuler
    - Kontrolgrupperne (og hvordan de udvælges)
    - "The plan, do, check, act" cyklus for kontinuerlige forbedringer.

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

Som et sidste led i it-revisionen (forvaltningsrevision) for 2019 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 forret-

nings-/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 disse ikke gennemgået governance –modellen.

Forvaltningsrevisionen har endvidere omfattet en overordnet gennemgang af nedennævnte områder:

- Overordnet gennemgang af Pædagogisk IT
- Leverandørstyring
- SharePoint.

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

Pædagogisk IT

Forvaltningsrevisionen af Pædagogisk IT har i 2019 omfattet en overordnet gennemgang på interview basis af Pædagogisk IT's (herefter PIT) ydelser, herunder en vurdering af, hvorvidt KK's IT-retningslinjer er implementeret hos PIT.

Pædagogisk IT 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.

PIT'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.

PIT råder over omkring 50 medarbejdere, hvor af 20 er udkørende teknikkere, som blandt andet varetager driftssupport.

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

PIT-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 PIT har været omfattet af KK's risikostyringsprojekt, således at der er foretaget en risikovurdering samt konsekvensanalyse af udvalgte områder i PIT. Yderligere har PIT gennemført en uafhængig risikovurdering af deres centrale netværksudstyr.

Hvad angår leverandørstyring, er det oplyst, at PIT anvender de rammeaftaler, som kommunen har implementeret. Alle PIT'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 PIT, som periodisk følger op på de indgåede aftaler.

Det er oplyst, at PIT'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 PIT's AD.

Endvidere har vi fået oplyst, at der er i forbindelse med, at STIL kommer med et nyt UNI-Login d. 18. februar 2020, hvor de ikke længere tilbyder password-synkronisering, har BUF's Direktion besluttet, at både elever og pædagogiske medarbejdere fremover skal anvende PIT's AD til login til AULA, læringsplatforme, digitale læremidler mv. således, at med denne beslutning implementerer PIT også password-politikker baseret på KK's krav.

I forbindelse med revisionen af 2020 vil vi foretage en stikprøvevis gennemgang af den faktisk implementerede sikkerhed hos PIT i form af konkrete test af adgange samt den opsatte sikkerhed.

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 2019 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 konstateret, at 11 ud af 12 observerede afvigelser er lukket i pågældende revisionsperiode. Det er oplyst, at den udestående afvigelse forventes lukket inden udgangen af 2019.

Vi vil følge op på denne, når systemrevisionserklæringen for 2019 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.

Det er oplyst, at projektet afrapporterer til it-kredsen hver 14. dag og afholder løbende styregruppemøder, hvor status fremlægges, og yderligere tiltag drøftes, aftales og godkendes.

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

Derudover er arbejdsgruppen fortsat i gang med gennemgang af rettighedsstyringen i SPO. Der er i forbindelse med denne gennemgang foretaget en stikprøvegennemgang af brugere og deres adgange og rettigheder.

Vi kan på baggrund af vores interviews samt modtaget dokumentation konstatere, at Københavns Kommune på nuværende tidspunkt ikke har været igennem alle data/filer/mapper, der er oprettet i SPO. Yderligere er en komplet gennemgang af samtlige brugere og deres rettigheder ikke gennemført på nuværende tidspunkt.

Det er oplyst, at der ikke er fastlagt endelige datoer for, hvornår projektet forventes at være i mål.

1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2019 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 fire revisionsbemærkninger samt fire revisionsbemærkninger, som vi har kunne lukke. Af de afgivne revisionsbemærkninger kan:

- To revisionsbemærkninger henføres til nye bemærkninger i forbindelse med den udførte it-revision
- To revisionsbemærkning henføres fra tidligere år til revisionen af årsregnskabet
- To revisionsbemærkninger (herudover er to observationer lukket) fra tidligere år vurderes lukket (overgået til to observationer) i forbindelse med den udførte revision

2.1. Revisionserklæringer

Der forventes modtaget primo 2020 revisionserklæring for de generelle it-kontroller omfattende KMD's generelle driftsydelser samt en specifik erklæring til KMD Kvantum og en specifik erklæring til KMD Opus.

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

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

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.1.1 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	En manglende eller utilstrækkeligt 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 efter planen.	2019

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
	overensstemmelse med databeskyttelsesfor-ordningens artikel 32.			

Organisationsområde i KK	BUF	Revisionsområde/ emne	Pædagogisk IT (PIT)

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.1.2 Pædagogisk IT	*Pædagogisk IT* Vi har konstateret, at PIT'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 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 PIT's AD. Endvidere har vi fået oplyst, at der er i forbindelse med, at STIL kommer med et nyt UNI-Login d. 18.februar 2020, hvor de ikke længere tilbyder password-synkronisering, har BUF's direktion besluttet, at både elever og pædagogiske medarbejdere fremover skal anvende PIT's AD til login til AULA, læringsplatforme, digitale læremidler mv. således, at med denne beslutning implementerer PIT også password-politikker baseret på KK's krav.	Manglende eller utilstrækkelige krav til password-opsætningen 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 på den oplyste løsning, således at PIT bliver underlagt det ønskede it-sikkerhedsniveau, som er fastlagt af KK.	2019

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, KMD Aktiv og Kvantum)** Vi har fået oplyst, at der ikke foretages en periodisk gennemgang af brugere og tildelte rettigheder i KMD Opus og KMD Aktiv, ligesom der ikke foretages en vurdering af funktionsadskillelsen i systemerne. Vedr. Kvantum har vi konstateret, at den periodiske revurdering alene er foretaget for brugere tilknyttet SAP Kompetencecentret og ikke for samtlige forvaltninger. **Fratrædelser (KMD Opus, KMD Aktiv, Kvantum)** Vi har fået oplyst, at den centrale brugeradministration ikke i alle tilfælde får besked om brugerfratrædelser eller rokader, hvor medarbejdere skal nedlægges i systemerne. Derudover har vi i forbindelse med vores stikprøvegennemgang af fratrådte brugere konstateret, at en række fratrådte brugere fortsat er aktive i KMD Opus, KMD Aktiv og KMD Kvantum. **Oprettelser (Kvantum)** Vi har i forbindelse med vores stikprøvegennemgang af brugeroprettelser i KMD Aktiv konstateret, at der ikke i alle tilfælde foreligger en oprettelsesanmodning/godkendelse. Det har således ikke været muligt at modtage dokumentation for 1/25 stikprøver til Kvantum. **Status 2019** *Periodisk revurdering -KMD Debitor, KMD Aktiv*	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 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 Opus, KMD Aktiv 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 netværk 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	2018 2019

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
	Vi har fået oplyst, at der ikke er foretaget en periodisk gennemgang af brugere og tildelte rettigheder i KMD Opus og KMD Aktiv, ligesom der ikke foretages en vurdering af funktionsadskillelsen i systemerne. Vi er dog bekendte med, at der i forhold til KMD Debitor, er igangsat et projekt med henblik på at vurdere de etablerede roller, herunder roller der kollidere 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 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, 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, KMD Aktiv og KMD Kvantum.		formelle og dokumenterede autorisationer.	

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 og KMD Debitor og tilhørende platforme. 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 KMD 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 Debitor. Der kan således være forhold og risici relateret til blandt andet ændringshåndteringen, som vi er ikke bekendt med. **Status 2019** Vi har konstateret, at der er igangsat en proces til lukning af de oplistede forbehold og bemærkninger i revisionserklæringerne. Der vil blive fulgt op på forholdene, når erklæringen for 2019 foreligger. Denne forventes primo 2020.	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 Debitor for at opnå en højere grad af sikkerhed. Endvidere vil vi følge op på, at der indhentes relevant revisionserklæring vedr. Kvantum for 2019 til sikring af, at de konstaterede forhold i 2018 er lukkede.	2017 2018 2019

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 It-risikoanalyse - Kvantum	Vi har konstateret, at KK har udarbejdet en risikoanalyse på Kvantum. Dog mangler forvaltningsdirektionen at godkende risikoappetitten og risikohåndteringsplanen. **Status 2019** Vi har konstateret, at risikoappetit og risikohåndteringsplaner er forelagt koncerndirektionen. Punktet lukkes.	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.		
3.3.2 Beredskabsplaner	Vi har fået oplyst, at KK er ved at afrunde projektet vedrørende udarbejdelsen af forretningsorienterede beredskabsplaner i de enkelte forvaltninger. Der er efter det oplyste nedsat en arbejdsgruppe, som har til opgave at tilpasse og fintune de udarbejdede beredskabsplaner. Derudover er det oplyst, at skrivebordstest er planlagt gennemført i Q2 2019. Observation opretholdes. **Status 2019** Vi har konstateret, at udarbejdelsen af forretningsorienterede beredskabsplaner er tilendebragt og godkendt. Yderligere har vi konstateret, at der er gennemført en samlet beredskabsøvelse med repræsenter fra de respektive forvaltninger. Punktet lukkes.	En manglende eller utilstrækkelig it-beredskabsplan medfører risiko for, it-systemer ikke kan genetableres som forventet i tilfælde af en sikkerhedshændelse.		

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 – Standard profiler med udvidede rettigheder	**SAP_ALL** Vi har konstateret, at fire personlige brugere er tildelt SAP_ALL rettigheder i KP5. Derudover har vi konstateret, at en personlig profil er tildelt SAP_ALL rettigheder på KPA. Yderligere har vi konstateret, at en række dialogbrugere er tildelt SAP_ALL rettigheder på KP0, KP5, KP6 samt KPA. Vi har endvidere konstateret, at et antal kommunikationsbrugere med SAP_ALL rettigheder er konfigureret med typen Dialog. *SAP* og DDIC* Vi har konstateret, at SAP standardbrugerne SAP* og DDIC ikke er blevet låst eller udløbet. **Status 2019** Vi har konstateret, at SAP_ALL rettigheder er fjernet fra ovenstående brugere og såfremt nødvendigt, alene tildeles på baggrund af formelle og godkendte anmodninger. *SAP* og DDIC* Vi har konstateret, at SAP standardbrugerne hos KMD for SAP* og DDIC ikke er blevet låst eller udløbet.	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

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

Ref.	Observationer	Risikobeskrivelse	Anbefalinger	Risiko og væsentlighed
3.4.2 Kvantum – Change management - Test	Vi har for Kvantum konstateret, at der ikke er stillet formelle krav til den gennemførte tests omfang, kvalitet og dokumentation. Yderligere har vi i forbindelse med vores stikprøvegennemgang af gennemførte ændringer konstateret, at der ikke i alle tilfælde foreligger dokumentation for gennemført test og testgodkendelse. **Status 2019** 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.	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.	Vi henstiller, at den implementerede forretningsgang gældende for 1. april følges fremadrettet, således at test af ændringer altid dokumenteres forud for idriftsættelse. For ændringer foretaget før 1. april henstiller vi til, at risikoen herved vurderes.	2018 2019

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

Ref.	Observationer	Risikobeskrivelse	Anbefalinger	Risiko og væsentlighed
3.4.3 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. 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 2019** Vi har fået oplyst, at det på baggrund af godkendelse fra IT-kredsen er besluttet, at risikorapporteringsprocessen inddrages i Kommunens obligatoriske uddannelse for både tekniske og forretningsansvarlige systemejere. Et endeligt	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.	For at kunne øge kenskabet til den nuværende risikorapporteringsproces, og for at fremhæve den positive indvirkning risikorapportering har på alle niveauer, anbefaler vi, at en risiko awarness workshop afholdes for de syv forvaltninger. Workshoppen bør fokusere på følgende områder: 1. Linket mellem en forretningsrisiko og en informationssikkerhedsrisiko 2. Risikoejerskab 3. Risikoidentifikation og rapportering 4. Risk management 5. Risikohåndtering i kontekst med SIEM 6. Praktisk risikodemonstration. Vi anbefaler, at der afholdes en ISO 27001 awarness workshop for de syv forvaltninger. Workshoppen bør fokusere på følgende områder: 1. Overblik over informationsmanagementsystemet (ISMS) 2. Betydningen af risici i ISMS 3. De obligatoriske klausuler 4. Kontrolgrupperne (og hvordan de udvælges) 5. "The plan, do, check, act"-	2018 2019

Ref.	Observationer	Risikobeskrivelse	Anbefalinger	Risiko og væsentlighed
	uddannelsesprogram forventes præsenteret for IT-kredsen samt DCK ultimo 2019. Vi har fået oplyst, at en ISO 27001 awarness workshop forventes afholdt i december 2019. Vi har fået oplyst, at der er afholdt et fællesmøde om logning af fagsystemer i SIEM med fokus på risikoejerskab og risikohåndtering (logopfølgning i fagsystemer) den 20. august 2019. Vi har fået oplyst, at KIT's monitoreringsgruppe i Kontoret for Operationel Sikkerhed i 2019 har udarbejdet og formidlet revideret materiale og vejledning om logning og logopfølgning til forvaltningerne.		cyklus for kontinuerlige forbedringer.	

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

Ref.	Observationer	Risikobeskrivelse	Anbefalinger	Risiko og væsentlighed
3.4.4 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 2019** Vi har konstateret, at der er gennemført ledelsestilsyn af brugeradgange og rettigheder til UiPath i august 2019. Vi har i forbindelse med vores stikprøvegennemgang indhentet og gennemgået testrapporter for to udvalgte robotter. Gennemgangen har ikke givet anledning til bemærkninger. Vi har stikprøvevis konstateret, at ansvarsfordelingen mellem KIT og forretningen er dokumenteret i de udarbejdede driftsaftaler. Vi har dog konstateret, at for implementering af robotter før KIT overtog styringen i forbindelse med kontroller omkring implementeringen, har disse ikke gennemgået governance –modellen På baggrund heraf opretholdes punktet.	En manglende eller utilstrækkeligt governance af automatiserede processer medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi anbefaler, at der indføres en formel periodisk gennemgang af tildelte adgange til UiPath Vi anbefaler, at udførte testhandling dokumenteres, og at de dokumenterede testhandlinger indgår i vurdering om, hvorvidt robotten er klar til produktion Vi anbefaler, at det præciseres i driftsaftalerne, hvem der er ansvarlige for, at overvåge input/output af robotterne (forretningsfejl). Vi anbefaler, at der laves en gennemgang af tidligere implementerede robotter for at sikre, at disse er underlagt governance-modellen.	2018 2019

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

Ref.	Observationer	Risikobeskrivelse	Anbefalinger	Risiko og væsentlighed
3.4.5 It-risikovurderinger	Vi har i perioden fra den 1. januar til den 19. december 2018 konstateret, at sikringsforanstaltninger i KIT's koncept for udarbejdelse af it-risikoanalyser/sikkerhedsvurderinger ikke er sammenholdt med annex A kontrollerne i ISO 27001. Vi har endvidere konstateret, at det ikke er fyldestgørende dokumenteret, hvordan sammenhængen er mellem den initiale risiko, og hvilke sikringsforanstaltninger som er vurderet relevante for systemet, og hvad den endelig risiko er, når sikringsforanstaltninger er medregnet. Endvidere har vi konstateret en svag/manglende ledelsesforankring på KK-niveau i forhold til at få fastsat risikoejerskab og risikotolerance. Vi har per den 20. december 2018 konstateret, at KIT har opdateret deres sikkerhedsvurderinger, således at: 1) de er koblet op på ISO 27001 standarden 2) der er sammenhæng mellem den initiale risiko og sikringsforanstaltninger, som er vurderet relevante, og hvad den endelig risiko er, når sikringsforanstaltninger er medregnet 3) det er kommunikeret til direktionen. Endvidere er det konstateret, at der foreligger færdige sikkerhedsvurderinger for 11 systemer, som er identificeret som de mest kritiske af økonomiforvaltningen. Dog mangler forvaltningsdirektionen at godkende risikoappetitten og risikohåndteringsplanen.	En manglende eller utilstrækkelig it-risikoanalyse medfører risiko for, at det etablerede it-sikkerheds-niveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	For 2019 udestår, at forvaltninger får lukket de af KIT fremsatte henstillinger vedrørende risikovurderingerne for 2018.	2018 2019

Ref.	Observationer	Risikobeskrivelse	Anbefalinger	Risiko og væsentlig-hed
	Status 2019 Vi har konstateret, at risiko-appetit og risikohåndterings-planer er forelagt koncern direktionen i september 2019. Dog er det konstateret, at der udestår, at forvaltnin-gerne får lukket de af KIT fremsatte henstillinger ved-rørende risikovurderingerne for 2018. På baggrund heraf opretthol-des punktet.			

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 Jesper Due Sørensen på telefon 3093 6420.

København, den 11. december 2019

Deloitte
Statsautoriseret Revisionspartnerselskab

Lars Kronow
statsautoriseret revisor

Jesper Due Sørensen
partner

NIEG/hakj
T:\Afd1180\Københavns Kommune\2019\Københavns Kommune - GIK rapport 2019 END 121219_1.docx