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 Peter Stensgaard Mørch
Københavns Rådhus
1599 København V

Revisionsrapport – Revision af generelle it-kontroller 2018

Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2018 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.

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 en årlig specifik erklæring til KMD Opus.

Forvaltningsrevision
Forvaltningsrevisionen har omfattet en vurdering af igangsatte aktiviteter inden for nedennævnte områder:

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

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

KIT's koncept for sikkerhedsvurderinger

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 2018 har vi gennemgået KIT's koncept for risikovurderinger.

Vi har konstateret, at koncept for it-sikkerhedsvurderinger/risikovurderinger har indarbejdet et trusselskatalog samt et katalog over sikringsforanstaltninger, som skal gennemgås for hvert system, hvor der skal udarbejdes en risikoanalyse. Det er vores vurdering, at trusselskataloget og kataloget over sikringsforanstaltninger giver et godt fundament til udarbejdelse af risikoanalyserne. I forhold til ISO

27001 rammeværket er KIT's kataloget over sikringsforanstaltninger ikke struktureret efter kontrolområderne fra annex A i ISO 27001.

Vi ser primært tre områder, hvor vi anbefaler en styrkelse af koncept for it-risikovurderinger:

- Vi anbefaler, at der udarbejdes en Statement of Applicability (SoA) med en begrundelse for eventuelle fravalgte annex A kontroller. I SoA dokumentet vurderes, hvorvidt en kontrol er relevant eller kan undlades ud fra en betragtning, om kontrollen er best practices, et lovligt-, et kontraktuelt- eller et forretningskrav.

- Vi anbefaler, at den initiale risiko, og hvilke sikringsforanstaltninger som er vurderet relevante for systemet, og hvad den endelig risiko er, når sikringsforanstaltninger er medregnet, dokumenteres. Derved opnås en risiko før og efter sikringsforanstaltninger er taget i betragtning. Det vil give mulighed for at få tydeliggjort, hvilken påvirkning den enkelte sikringsforanstaltning har på risikoen.

- Endvidere anbefaler vi, at risikoanalysen får større ledelsesforankring på KK niveau. Risikovurderingen bør altid godkendes af det relevante ledelsesniveau. Risikohåndteringsplanen kan i praksis benyttes som en anbefaling/indstilling fra informationssikkerhedsudvalget til ledelsen. Her anføres det, hvilke tiltag som bør indføres, og hvilke risici som bør accepteres med udgangspunkt i de fastsatte kriterier for risikotolerance. Selvom risici reduceres ved at indføre yderligere kontroller, vil der i de fleste tilfælde altid være en restrisiko. Det er vigtigt, at der i risikohåndteringsplanen foretages en vurdering af de valgte kontrollers effekt på risikoen, og at den tilbageværende risiko vurderes og beskrives, og at ledelsen godkender dette, da risikotolerance bør være afstemt på relevant ledelsesniveau.

Rettighedsstyring i E-doc

Deloitte har i forbindelse med 2018 revisionen foretaget en gennemgang af forretningsgangen for styring af brugerrettigheder i E-doc. Vi har endvidere i E-doc stikprøvevist inspiceret på sags- og gruppeniveau, at tildelte rettigheder i E-doc var i overensstemmelse med rekvirerede rettigheder. I forbindelse med vores inspektion af rettigheder på sags- og gruppeniveau fandt vi ingen afvigelser. Vi konstaterede, at der i forretningsgangen for rettighedsstyring i E-doc, lægges op til, at det er de enkelte autorisationsansvarlige i forvaltningerne, som skal sikre, at der foretages en periodisk revurdering af tildelte rettigheder. Dog er der ingen opfølgning på, om de autorisationsansvarlige også har udført den periodisk revurdering, og ved forespørgsel hos udvalgte autorisationsansvarlige har det ikke været muligt at fremfinde dokumentation på, at de periodiske revurderinger af brugerrettigheder i E-doc var udført.

Vi anbefaler således, at der oprettes en formel kontrol til periodisk revurdering af brugerrettigheder, og at kontrollen får tildelt en central kontrolejer. Kontrollen kunne med fordel placeres i Koncernservice Brugeradministration, som kunne have ansvaret for, at de enkelte autorisationsansvarlige i forvaltningen gennemfører deres periodiske revurdering.

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 2018 har Deloitte gennemgået KIT's governance-model for SIEM, og vi har identificeret 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, anbefales det, at en risiko awareness 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 informations-sikkerhedshåndtering. 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.

- En af de udfordringer, som SIEM monitoreringsteamet står overfor, er, at der ikke er en god forståelse på kontorchefniveau af, hvad SIEM-monitoreringen gør, og hvorfor det er vigtigt. Vi anbefaler derfor, at der ligeledes gennemføres en workshop eller præsentation af SIEM-monitoreringsteamets ansvar og formål for forvaltningerne

- Et af de vigtigste områder i forhold til at forbedre modenheden af informationssikkerhedsniveauet (i dette tilfælde SIEM) er den dokumentation og de retningslinjerne, 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. Vi anbefaler således, at der foretages en detaljeret revurdering af dokumentationen og retningslinjerne, som understøtter SIEM-løsningen, med det formål at få opbygget den korrekte struktur og få maximeret udbyttet af dokumentationen.

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

Som et sidste led af it-revisionen (forvaltningsrevision) for 2018 har vi foretaget en revisionen af 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 leveranceansvar-lige. Det er i styregruppen, at beslutninger om de rette projektdeltagere, økonomi og ændringer til forretnings-/robotprocessen træffes. Kerneteamet er 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 fuldtids operatør. 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.

Vi ser primært tre områder, hvor vi anbefaler en styrkelse af forretningsgangene for udvikling og drift af robotter/automatiserede processer:

- En styrket kontrol af, hvem der har adgang til uiPath i form af en formel periodisk gennemgang af tildelte adgange
- At udførte testhandlinger dokumenteres, og at de dokumenterede testhandlinger indgår i vurdering af, hvorvidt robotten er klar til produktion
- At det præciseres i driftsaftalerne, hvem der er ansvarlige for at overvåge input/output af robotterne (forretningsfejl).

1.3. Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2018 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 3 revisionsbemærkninger samt tre revisionsbemærkninger, som vi har kunne lukke. Af de afgivne revisionsbemærkninger kan:

- Tre revisionsbemærkninger henføres til en ny bemærkning i forbindelse med den udførte it-revision
- Ingen revisionsbemærkninger henføres fra tidligere år til revisionen af årsregnskabet
- Ingen revisionsbemærkninger fra tidligere år vurderes helt lukket i forbindelse med den udførte revision
- Ingen revisionsbemærkninger henføres til andre bemærkning i forbindelse med forvaltningsrevision.

2.1. Revisionserklæringer

Der modtages primo 2019 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 delvist 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	Økonomiforvaltningen (ØKF)	**Revisionsområde/ emne**	Generelle it-kontroller og udvalgte områder til forvaltningsrevision

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.1.1 Styring af brugerrettigheder og systemadgange	**Periodisk revurdering (KMD Opus, KMD Aktiv, Kvantum og E-doc)** Vi har fået oplyst, at der ikke foretages en periodisk gennemgang af brugere og tildelte rettigheder i KMD Opus, KMD Aktiv og E-doc, 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 (KMD Aktiv)** 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 4/25 stikprøver til 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 funktions-adskillelsen i KMD Opus, KMD Aktiv, Kvantum og E-doc således, at der på baggrund af en konkret risikovurdering udarbejdes en oversigt over roller/adgangsrettighede r, der - ud fra ønsket om opretholdelse af en organisatorisk funktionsadskillelse - ikke bør tildeles til samme brugere. Yderligere henstiller vi, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere i KMD Opus, KMD Aktiv, Kvantum og E-doc. 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 brugeradministrationspr oceduren følges, således at tildeling af rettigheder til brugere sker på baggrund af formelle og dokumenterede autorisationer.	

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

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.1.2 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 den personlige profil Z8QGB 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 standard-brugerne SAP* og DDIC ikke er blevet låst eller udløbet.	Ved ikke at begrænse brugere, der har fået tildelt SAP_ALL i produktionen, forøges risikoen for uautoriserede ændringer til systemet, data mv., da SAP_ALL giver ubegrænset adgang til SAP.	Vi henstiller, at SAP_ALL fjernes fra alle brugere, undtagen dedikerede nødbruger-ID'er. Vi henstiller, at kommunikationsbrugere ændres til typen Kommunikation eller System. Vi henstiller, at SAP* og DDIC låses for at reducere risikoen for misbrug.	
3.1.3 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.	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 der i forbindelse med alle ændringer til idriftsættelse sker dokumentation af den gennemførte tests omfang og kvalitet.	

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

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

Ref.	**Observation**	**Risikobeskrivelse**	**Anbefaling**	**Risiko og væsentlighed**
3.2.1 It-sikkerhedsvurderinger	Vi har fået oplyst, at KK i samarbejde med PwC har foretaget en modenhedsanalyse, som har resulteret i en risikostyringsmodel, der beskriver de aktiviteter, som skal udføres for at skabe et samlet risikobillede. Risikostyringsmodellen er forelagt til bestyrelsens godkendelse. KK forventer, at risikoanalyser for de enkelte forvaltninger udarbejdes i løbet af 2015. **Status 2018** Vi har i perioden fra den 1. januar til den 19. december 2018 konstateret, at sikringsforanstaltninger i KIT's koncept for udarbejdelse at 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, 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.	Vi har i perioden 1. januar til 18. december anbefalet, at 1) sikkerhedsvurderinger knyttes til ISO 27001 standarden 2) risikoanalysen får større ledelsesforankring på KK niveau. Vi anbefaler, at der kommer større sammenhæng mellem den initiale risiko, og hvilke sikringsforanstaltninger som er vurderet relevante for systemet, og hvad den endelige risiko er, når sikrings-foranstaltninger er medregnet. Derved opnås en risiko før og efter sikringsforanstaltninger er taget i betragtning. Det vil give mulighed for at få tydeliggjort, hvilken påvirkning den enkelte sikringsforanstaltning har på risikoen. KK har efterfølgende korrigeret forholdet, da de opdaterede sikkerhedsvurdering for de mest kritiske systemer identificeret af Økonomiforvaltningen foreligger per 20. december 2018. Dog anbefaler vi, at forvaltningsdirektionen godkender risikoappetitten og risikohåndteringsplanen.	

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

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.2.2 Beredskabsplaner	Vi har konstateret, at it-beredskabsplanen for KK ikke har været opdateret siden 2015. Dette begrundes med, at KK har sat opdateringsarbejdet af beredskabsplanen i bero, da overvejelser af, hvilke tiltag der skal tages for at styrke og omorganisere beredskabsplanen, er igangværende. Derudover er det oplyst, at KK i 2017 har haft fokus på udarbejdelse af beredskabsplaner i de enkelte forvaltninger. Projektet er igangværende og således ikke fuldført. **Status 2018** 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.	En manglende eller utilstrækkelig it-beredskabsplan medfører risiko for, it-systemer ikke kan genetableres som forventet i tilfælde af en sikkerhedshændelse.	Vi anbefaler, at grundlaget for og formålet med beredskabsplanlægningen for de enkelte forvaltninger fastlægges og godkendes formelt af ledelsen, samt at opfyldelsen af kravene pr. system og platform efterfølgende dokumenteres og rapporteres til ledelsen. Yderligere anbefaler vi, at beredskabsplaner opdateres periodisk - minimum en gang årligt samt når andre faktorer indikerer nødvendigheden heraf.	

3.2.3 Revisionserklæringer	Københavns Kommune har indgået aftale med KMD omkring drift af KØR og Kvantum og tilhørende platforme. Der modtages årligt en revisionserklæring for de generelle it-kontroller, omfattende KMD's generelle driftsydelser. Vi har af KMD's revisor fået bekræftet, at Kvantums infrastruktur er omfattet af KMD's generelle driftsydelser. Dog henstiller vi, at der indhentes en specifik revisionserklæring for Kvantum for at opnå en højere grad af sikkerhed. KMD's revisor har endvidere oplyst, at KØR ikke er omfattet af KMD's generelle driftsydelser, og at der ikke er afgivet en specifik erklæring for KØR. Der kan således være forhold og risici relateret til den generelle drift af KØR i 2017, som vi ikke bekendt med. **Status 2018** Vi har konstateret, at Københavns Kommune har anmodet deres leverandør om årligt at afgive en revisionserklæring for de generelle it-kontroller omfattende KMD's generelle driftsydelser samt en årlig specifik erklæring til KMD Kvantum. Vi har endvidere konstateret, at der hvert andet år indhentes en specifik erklæring til KMD Opus. Vi forventer at kunne lukke punktet, når revisionserklæringer for 2018 foreligger	En manglende eller utilstrækkelig overvågning af underleverandører medfører risiko for, at underleverandører ikke efterlever det forventede it-sikkerhedsniveau.	Vi forventer at kunne lukke punktet, når revisionserklæringer for 2018 foreligger Vi forventer at kunne lukke punktet, når revisionserklæringer for 2018 foreligger.	

3.3. Bemærkninger 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-sikkerhedspolitik og it-sikkerhedsregler	Vi har konstateret, at KK's it-sikkerhedspolitik samt underliggende, uddybende it-sikkerhedsregler ikke er gennemgået og reviewet siden 2013. Det er yderligere oplyst, at sikkerhedspolitikker er planlagt til revidering i Q1 2018. **Status 2018** Vi har konstateret, at KK's it-sikkerhedspolitik samt regulativ for sikkerhedsregler er revurderet og omskrevet. Sikkerhedspolitikkerne er endvidere godkendt af Borgerrepræsentationen i juni 2018. Punktet lukkes.	En manglende eller utilstrækkeligt it-sikkerhedspolitik medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi har ingen anbefaling, da forholdet vurderes udbederet.	

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.3.2 Sikkerhedsprogram	PwC har i 2014 vurderet, at Københavns Kommunes modenhed på daværende tidspunkt var mangelfuld på en række centrale områder. I en opfølgende måling i 2016 er det vurderet, at der er sket en øget modenhed på de områder, hvor der er gennemført særlige tiltag, men at der samtidig var en del forbedringspunkter. På baggrund heraf har Københavns Kommune udarbejdet et sikkerhedsprogram, som skal medvirke til et generelt løft af it-sikkerhedsarbejdet i kommunen. Der bliver i sikkerhedsprogrammet foreslået ni indsatsområder, som der arbejdes videre med, enten som allerede igangsatte tiltag eller organiseret som nye projekter. **Status 2018** Vi har fået oplyst, at KK's Sikkerhedsprogram blev afsluttet i juni 2018. For enkelte områder videreføres arbejdet som selvstændige aktiviteter. Punktet lukkes.	Et manglende eller utilstrækkeligt it-sikkerhedsprogram medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi har ingen anbefaling, da forholdet vurderes udbederet.	
3.3.3 IT-governance	I revisionsrapporten for 2016 påpeger Intern Revision (IR), at der reelt mangler governance på it-området. IR anbefaler: • At governance skal fastlægges i en række standardiserede styringsregler og retningslinjer for anskaffelser • At der sker en entydig placering af beslutningsansvaret som en integreret del af kommunens strategiske ledelsesarbejde • At der arbejdes med en risikobaseret tilgang til styring af it-sikkerhed og it-governance • At der etableres en it-kreds til håndtering af den ledelsesmæssige forankring. Det er her afgørende, at topledelsen er repræsenteret i kredsen.	En manglende eller utilstrækkelig governance på it-området medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi henstiller, at arbejdet med en styrket IT governance-model forsættes og gennemføres efter planen	

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.3.3 IT-governance	Vi har i forbindelse med vores revision 2017 konstateret, at kommunen har udarbejdet en indstilling til styrket it-governance på it- og persondataområdet, samt at it-governance-modellen trådte i kraft den 1. januar 2018 med en række initiativer, der skal etableres i løbet af andet halvår 2018: • Etablering af en it-kreds på tværs af kommunens forvaltninger • Tværgående strategier • Klar rolle- og ansvarsfordeling i it-anskaffelsesprocesser. Vi er informeret om, at it-kredsens arbejdsprogram vil blive forelagt kredsen af administrerende direktører til godkendelse i 1. kvartal 2018. Et cirkulære for it-anskaffelser i KK forelægges for ØU i 2. halvår 2018. Cirkulæret erstatter den gældende anskaffelsesvurderingsproces fra 2012. En samlet redegørelse med fokus på varetagelse af it-sikkerhedsområdet forelægges for ØU og BR ved udgangen af 1. halvår 2018. Der udarbejdes en samlet status på it-kredsens arbejde i slutningen af 2018 til forelæggelse for ØU. Status 2018 Vi er informeret om at: • Der er udarbejdet et arbejdsprogram for it-kredsen for 2018, som blev godkendt af kredsen af administrerende direktører d. 22. februar 2018 • Der er udarbejdet et cirkulære for it-anskaffelser, som blev godkendt af BR d. 1. november 2018, og som nu gælder for alle anskaffelser. Cirkulæret fastsætter ansvarsfordeling mellem Økonomiforvaltningen og fagforvaltningerne ifm. anskaffelser og vil i 2019 blive understøttet af en fællesadministrativ forretningsgang på området. Ligeledes udarbejdes i 2019 yderligere cirkulære for drift, vedligehold og udfasning af systemer • Der er i 2018 udarbejdet status for 2017 til ØU om KK's it-sikkerhed, og ifm. budgetvedtagelsen af budget 2019 er der afsat midler til at styrke it-sikkerheden på cyberområdet gennem både en række tekniske og organisatoriske tiltag. • Der er udarbejdet en status til ØU på it-kredsens arbejde, som er godkendt af kredsen af administrerende direktører d. 13. december 2018. Sagen forelægges for ØU d. 8. januar 2019. Punktet lukkes		Vi har ingen anbefaling, da forholdet vurderes udbederet.	

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.3.4 Datasikkerhed	Vi har fået oplyst, at datatransport for så vidt angår persondata og værdidata altid skal foregå ved krypteret trafik, og at data på fysiske diske og USB (beskyttet med password) sendes med personlig overdragelse, og at der indhentes kvittering for modtagelse. Endvidere har vi observeret, at der ikke sker nogen systematisk opfølgning på, om medarbejdere i modstrid med reglerne opbevarer persondata på bærbare computere, og at data på disse computere ikke er krypteret. Endelig er det konstateret, at der hidtil ikke har foreligget retningslinjer for styring af mobile enheder (telefoner og tablets), men at sådanne retningslinjer, startende i oktober 2015, er under indførelse i forbindelse med det såkaldte "AirWatch-projekt". Vi har endvidere konstateret, at der er implementeret en procedure for bortskaffelse af informationsbærende medier, samt at der er igangsat et projekt, hvor Windows 7 skal udskiftes med Windows 10, og i den forbindelse vil harddiske blive krypteret. For mobile enheder er AirWatch etableret, og der er udarbejdet formelle retningslinjer. Vi har fået oplyst, at implementering af Windows 10 Enterprise med Bitlocker er påbegyndt i februar 2018 og forventes afsluttet omkring Q3 2018. Herved vil kommunen sikre kryptering af alle harddiske. **Status 2018** Vi har er informeret om, at implementering af Windows 10 Enterprise med Bitlocker er implementeret. Herved har kommunen sikret kryptering af alle harddiske. Punktet lukkes.	En manglende eller utilstrækkelig datasikkerhed medfører risiko for, at det etablerede it-sikkerhedsniveau ikke i tilstrækkeligt omfang imødegår de risici, som vurderes som relevante.	Vi har ingen anbefaling, da forholdet vurderes udbederet.	

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 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.	En manglende eller utilstrækkeligt 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 awareness 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 awareness 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" cyklus for kontinuerlige forbedringer. Vi anbefaler, at der ligeledes gennemføres en workshop eller præsentation af SIEM-monitoreringsteamet for de syv forvaltninger. Vi anbefaler, at der foretages en detaljeret revurdering af dokumentationen og retningslinjerne, som understøtter SIEM-løsningen med det formål at få opbygget den korrekte struktur og få maximeret udbyttet af dokumentationen.	

Ref.	Observation	Risikobeskrivelse	Anbefaling	Risiko og væsentlighed
3.4.2 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.	En manglende eller utilstrækkeligt governance af automatiserede processer medfører risiko for, at det etablerede it-sikker-hedsniveau 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 testhandling 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).	
3.4.3 It-risikoanalyse - Kvantum	Vi har konstateret, at KK i 2017 har iværksat en proces med henblik på vurdering og udvælgelse af fagsystemer, som skal indgå i det påbegyndte risikovurderingsprojekt, hvor fokus primært er på systemer, som indeholder personfølsomme data. Desuden er det konstateret, at det nye Kvantum-system ikke har været omfattet af udvalgte systemer. Det er endvidere oplyst, at der i forbindelse med idriftsættelse af systemet i 2017 er udarbejdet ibrugtagningstilladelse, hvori systemet er godkendt på baggrund af en overordnet risikovurdering. Prioritering vil være gul for denne. **Status 2018** Vi har konstateret, at KK har udarbejdet en risikoanalyse på Kvantum. 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.	Vi anbefaler, at forvaltningsdirektionen godkender risikoappetitten og risikohåndteringsplanen.	

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 adgang 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 30 93 64 20.

København, den 14. februar 2019

Deloitte
Statsautoriseret Revisionspartnerselskab

Lars Kronow
statsautoriseret revisor

Jesper Due Sørensen
partner

JHON/hakj/as
T:\Afd1180\Københavns Kommune\2019\Københavns Kommune GIK-rapport END 120219.docx