Sharepoint ●	**Rettet mod: Forvaltningerne**	**Omtalt år: 2019**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Sharepoint Vi har konstateret, at Københavns Kommune primo 2019 har gennemført en risikovurdering samt en konsekvensanalyse af Microsoft SharePoint Online og brugen heraf med henblik på at vurdere, hvorvidt der er behov for at iværksætte yderligere tekniske eller organisatoriske sikringsforanstaltninger for at beskytte personoplysninger og værdidata. I forlængelse af risikovurderingsprojektet er der konstateret områder, hvor forbedrende tiltag er iværksat. Sideløbende med det er der igangsat et forvaltningsfælles oprydningsprojekt, som blandt andet har til formål, at vurdere og klassificere data i SPO, vurdere rettighedsstyringen, herunder definere dataejere samt vurdere og gennemgå adgange til data. Det er yderligere oplyst, at der ikke er fastlagt endelige datoer for, hvornår projektet forventes afsluttet. Der er fra Datatilsynet truffet afgørelse i sagen, som retter følgende afgørelse: Efter en gennemgang af sagen finder Datatilsynet grundlag for at udtale alvorlig kritik af, at Københavns Kommunes behandling af personoplysninger ikke er sket i overensstemmelse med databeskyttelsesforordningens artikel 32. **Risici** 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.	**[angiv forvaltningens handleplan]** Beskæftigelses og integrationsforvaltningen direktionsbehandler oprydningsprojektet i januar 2020. Forvaltningen forventer at have gennemført oprydningsprojektet inden 1.5.2020.

Styring af brugerrettigheder og systemadgange ●	Rettet mod: Økonomiforvaltningen og Beskæftigelsesforvaltningen	Omtalt år: 2018 og 2019
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
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* 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	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 formelle og dokumenterede autorisationer.	**[angiv forvaltningens handleplan]** Vurdering af funktionsadskillelsen i KMD Aktiv er i proces. Ligeledes foretages der periodisk og dokumenteret revurdering af tildelte rettigheder til brugerne i KMD Aktiv i 2020. Brugeradministrationen i KS vil igen blive anmodet om at følge gældende retningslinjer for tildeling og nedlæggelse af brugere i KMD Aktiv. Revisorerklæring rekvireres hvert år i marts/april måned fra leverandøren.

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. **Risici** Manglende eller utilstrækkelig kontrol med system-rettigheder 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.		

It-risikovurderinger ●	**Rettet mod: Økonomiforvaltningen**	**Omtalt år: 2018 og 2019**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
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. **Status 2019** Vi har konstateret, at risikoappetit og risikohåndteringsplaner er forelagt koncerndirektionen i september 2019. Dog er det konstateret, at der udestår, at forvaltningerne får lukket de af KIT fremsatte henstillinger vedrørende risikovurderingerne for 2018. På baggrund heraf opretholdes punktet.	For 2019 udestår, at forvaltninger får lukket de af KIT fremsatte henstillinger vedrørende risikovurderingerne for 2018.	**[angiv forvaltningens handleplan]** Forvaltningen har haft løbende dialog med KIT omkring risikovurderingerne og det vurderes, at der er udført handlinger på alle fremsatte henstillinger, og dermed ingen udeståender.

Risici 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.		