Bilag 2 – Handleplaner revisionsrapport generelle it-kontroller

Outsourcing-leverandørstyring - Gul
Økonomiforvaltningen

Observationer	Risikobeskrivelse	Anbefaling	Handleplan
Outsourcing-anskaffelsesprocedure og retningslinjer for leverandørstyring Vi har konstateret, at IT-anskaffelser og kontraktindgåelser for ældre systemer ikke følger Københavns Kommunes Governance-model herfor. Yderligere har vi konstateret, at der ikke foreligger klare retningslinjer for leverandørstyring, som er gældende på tværs af alle forvaltninger. Processen er forankret i de enkelte forvaltninger, hvilket gør, at monitorering og opfølgning ikke sker i tilstrækkelig grad.	Manglende eller utilstrækkelig styring og monitorering af leverandører medfører risiko for, at de leverede ydelser ikke dækker forretningsmæssige behov, samt at leverandører ikke efterlever det forventede ITsikkerhedsniveau.	Vi henstiller, at leverandørkontrakter undergår Københavns Kommunes Governance-model ved genforhandling. Derudover henstiller vi, at der etableres fælles administrative forretningsgange for opfølgning og monitorering af leverandørydelser.	Københavns Kommune har været i dialog med Ekstern revision om bemærkningen. Fokus for handleplanen er de *it-sikkerhedsmæssige* forhold for outsourcede it-løsninger. Til håndtering af dette, vil KIT i 2022 revurdere de eksisterende retningslinjer for it-sikkerhedskrav ved outsourcede løsninger og sikre, at KK har fælles retningslinjer for krav, der stilles til leverandører og deres underleverandører. På den baggrund vil KIT i it-kredsen (ITK) indstille, at der etableres en fællesadministrativ forretningsgang for retningslinjer, opfølgning og monitorering af leverandørydelser. Parallelt hermed er Koncern IT ved at professionalisere systemejerområdet med tværgående anbefalinger og processer for god praksis. Her vil der overfor systemejerne være et stort fokus på leverandørsamarbejdet og compliance med de krav, der er indgået med leverandørerne. Deadline: Q3 2022

Styring af roller og rettigheder – Kvantum - Rød
Økonomiforvaltningen

Observationer	Risikobeskrivelse	Anbefaling	Handleplan

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. **Status 2021** Vi har konstateret, at forholdet fortsat er uændret, og der således ikke er implementeret en centraliseret løsning mhp. at sikre, at ledelsestilsyn udføres på tværs af forvaltningerne. Vi har dog fået oplyst, at forholdet forventes udbedret i 2022 i forlængelse af nye, smallere roller til Kvantum, der samtidigt udføres ledelsestilsyn i forvaltningerne og centralt ledelsestilsyn,	Manglende eller utilstrækkelig kontrol med systemrettigheder og systemadgange til brugere medfører en øget risiko for, at brugeradgange misbruges, samt at brugeres rettigheder bliver utidssvarende og ikke afspejler deres arbejdsmæssigt betingede behov.	Vi henstiller, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere i Kvantum.	Centralt ledelsestilsyn (via IGA-løsningen) forventes gennemført i august 2022 i umiddelbar forlængelse af implementering af nye, smallere roller til Kvantum. Baggrunden herfor er, at projektet vedrørende nye smallere roller er blevet forsinket grundet frozen zone august-november 21 (Kvantum migrering) og efterfølgende frozen zone (årsafslutning) december 21 – januar 2022. De nye, smallere roller er designet og afventer alene organisatorisk implementering. I forbindelse med nedlæggelse af de eksisterende roller og tildeling af de nye, smallere roller til alle Kvantum brugere med deadline juli 2022 udføres samtidigt ledelsestilsyn i forvaltningerne og centralt ledelsestilsyn fra KS' side herpå. Deadline: 31. august 2022

Revisionserklæringer - Gul

Økonomiforvaltningen

Observationer	Risikobeskrivelse	Anbefaling	Handleplan
Københavns Kommune har indgået aftale med KMD	En manglende eller utilstrækkelig	Vi henstiller, at der indhentes en specifik	Der udarbejdes fra og med 2021 specifikke

omkring drift af Kvantum, KMD Aktiv, KMD Opus Debitor, KMD Opus Løn og tilhørende platforme. 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 vedrørende 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 Opus Debitor eller KMD Opus Løn. Der kan således være forhold og risici relateret til blandt andet ændringshåndteringen, som vi er ikke bekendt med. **Status 2021** Vi har fået oplyst, at Københavns Kommune har rekvireret specifikke systemrevisionserklæringer for Kvantum, KMD Opus Debitor og KMD Opus Løn. Disse forventes modtaget primo 2022. Der vil blive fulgt op på forholdende, når erklæringerne foreligger. Observationen nedprioriteres og forventes lukket i forbindelse med revisionen af 2022.	overvågning af underleverandører medfører risiko for, at underleverandører ikke efterlever det forventede IT-sikkerhedsniveau.	revisionserklæring for KMD Opus Debitor og KMD Opus Løn for at opnå en højere grad af sikkerhed.	erklæringer af typen ISAE 3402, type 2 gældende for Kvantum, Opus Debitor og Opus Løn. På baggrund af revisionens ønske omfatter erklæringen fra 2021 ligeledes applikationskontroller. Disse er i foråret 2021 fastlagt på møder mellem KK's revisorer og leverandørens revisor. Applikationskontroller indgår første år dog kun fra tidspunkt for design og året ud. Deadline: 31. marts 2022

BUF it-drift - Gul

Børne- og Ungdomsforvaltningen

Observationer	Risikobeskrivelse	Anbefaling	Handleplan
BUF IT-drift Vi har konstateret, at BIT's AD er baseret på UNI-Loginoplysninger fra Styrelsen for It og Læring (STIL). Endvidere	Manglende passwordskift medfører risiko for, at det ønskede IT-sikkerhedsniveau ikke i tilstrækkeligt omfang	Vi henstiller, at der arbejdes videre med implementeringen af periodisk passwordskift, således at løsningen bliver	Tvunget passwordskifte implementeres sammen med NSIS-projektet, som er den nye nationale standard for identiteters

er det oplyst, at STIL aldrig har haft en implementeret passwordpolitik på UNILogin. Brugerne (elever og pædagogiske medarbejdere) skal selv stå for at skifte deres passwords med jævne mellemrum. Det ændrede password bliver synkroniseret til BIT's AD. Endvidere har vi fået oplyst, at BUF's direktion (i forbindelse med, at STIL kommer med et nyt UNI-Login den 18. februar 2020, hvor de ikke længere tilbyder passwordsynkronisering) har besluttet, at både elever og pædagogiske medarbejdere fremover skal anvende BIT's AD til login til AULA, læringsplatforme, digitale læremidler mv., således, at man med denne beslutning også implementerer BIT's passwordpolitikker baseret på KK's krav. **Status 2021** Vi har konstateret, at der ikke er opsat tvunget periodisk skift af password for brugere, som tilgår BIT's AD baseret på Københavns Kommunes generelle krav til passwordpolitik. Vi er oplyst om, at denne forventes implementeret i forbindelse med implementeringen af den nye nationale standard NSIS, hvor BUF ITdrift er en del af NSIS-projektet. Punktet opretholdes.	imødegår de risici, som vurderes som relevante.	underlagt det ønskede IT-sikkerhedsniveau, som er fastlagt af Københavns Kommune.	sikringsniveauer (NSIS), som har til formål at skabe større tillid til digitale identiteter og digitale ID-tjenester. BUFs pædagogiske Azure AD (IdP) som rummer alle pædagogiske medarbejdere skal godkendes til NSIS niveauet LAV. BUF IT-drift er en del af NSIS-programmet i KK. I samarbejde med Koncern IT er der valgt en teknisk løsning, der allerede gør brug af eksisterende cloudbaseret teknologi, således at BUFs IdP kan valideres med NemID og på sigt MitID. Da løsningen potentielt er udfordret af Schrems II dommen vil BUF nu drøfte løsningen med kommunens DPO. Afhængig af DPO'en konklusioner, så forventes det, at løsningen sættes i drift i 1. halvår af 2022, og dermed implementering af tvungen password skift for pæd. medarbejdere.

Kvantum Standardprofiler med udvidede rettigheder - Rød

Økonomiforvaltningen

Observationer	Risikobeskrivelse	Anbefaling	Handleplan

SAP og DDIC* Vi har konstateret, at SAPstandardbrugerne hos KMD for SAP* og DDIC er aktive, men at de kun kan tilgås via secure server hos KMD. Vi har gennemgået loggen over anvendelsen og kan konstatere, at SAP* ikke har været anvendt i perioden, samt at DDIC har været anvendt i forbindelse med patchning i starten af revisionsperioden. Endvidere har vi konstateret, at der pr. januar måned er lavet aftale med KMD om deaktivering af de to brugere. Samtidigt er der opsat en ny proces for aktivering og anvendelse af de to brugere, hvor der kræves case-bycase review af anvendelsen. Vi vil efterteste denne proces i forbindelse med næste års revision. Baseret på den fremlagte roces forventer vi at kunne lukke punktet i forbindelse med næste års revision. **Status 2021** Vi har konstateret, at serviceleverandøren KMD i perioden fra januar 2021 til 1. april 2021 har haft adgang til Kvantum produktionsmiljøet med standardbrugere SAP* og DDIC. Vi har i forbindelse med vores IT-revision konstateret, at brugerne	Manglende eller utilstrækkelig sikkerhed for SAPstandard superbrugere SAP* og DDIC forøger risikoen for, at disse bruger-ID'er anvendes til at opnå uautoriseret adgang til SAP, da disse bruger-ID'er er oplagte mål for indtrængere.	Fra april 2021 er brugerne lukket, og bemærkningen er dermed lukket fra 1. april 2021.	Bemærkningen er lukket den 1. april 2021.