Koncern IT
Økonomiforvaltningen

Bilag

Til Økonomiudvalget

Bilag 2 – Handleplaner generelle it-kontroller 2020

8. februar 2021

Sagsnummer
2021-0022238

Dokumentnummer
2021-0022238-2

3.2.1 Styring af brugerrettigheder og systemadgange	**Rettet mod: Økonomiforvaltningen, Beskæftigelses-Integrationsforvaltningen**	**Omtalt år: 2018, 2019, 2020**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Periodisk revurdering – KMD Opus Debitor, KMD Opus Løn, KMD Aktiv: Deloitte har fået oplyst, at der fortsat ikke er foretaget en periodisk revurdering af tildelte rettigheder for brugere oprettet i KMD Aktiv, ligesom der ikke er foretaget en vurdering af funktionsadskillelsen i systemet. For så vidt angår KMD Opus Debitor Deloitte fået oplyst, at autorisationsprojektet fortsat er igangværende og at deadline for projektet er sat til 31/3-2021. Derudover er der ikke etableret en procedure for periodisk gennemgang af tildelte rettigheder til brugere i KMD Opus Løn, ligesom den månedlige funktionsadskillelseskontrol vedrørende indberetninger ikke er foretaget konsistent i revisionsperioden. *Periodisk revurdering – Kvantum:* Deloitte har fået oplyst, at forholdet fortsat er uændret. Deloitte har endvidere fået oplyst, at der er igangsat et projekt med henblik på at implementere en centraliseret løsning for den periodiske revurdering	Deloitte henstiller, at der foretages en formel vurdering af funktionsadskillelsen i KMD Opus Debitor og KMD Aktiv således, at der på baggrund af en konkret risikovurdering udarbejdes en oversigt over roller og adgangsrettigheder, der ud fra ønsket om opretholdelse af en organisatorisk funktionsadskillelse ikke bør tildeles samme brugere. Deloitte henstiller, at der periodisk foretages en dokumenteret revurdering af tildelte rettigheder til brugere i KMD Aktiv og Kvantum. Deloitte 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. Deloitte henstiller, at brugeradministrationsproceduren følges, så tildeling af rettigheder til brugere sker på baggrund af formelle og dokumenterede autorisationer.	*Periodisk revurdering – KMD Aktiv:* KMD Aktiv udfases i 2. halvår 2021, jf. planerne for overgang til KY. Periodisk revurdering, foruden de allerede etablerede kontroller, er svært at imødekomme inden udfasning. Det er ikke i KMD Aktiv muligt at funktionsadskille brugeren der opretter ydelsen fra brugeren, der godkender ydelsen, da brugerprofilerne ikke giver denne mulighed. For at imødekomme problematikken er forvaltningerne autorisationsmæssigt adskilt, så der ikke kan laves udbetalinger mellem forvaltningerne og dermed ikke til andre enheder, end dem der er tildelt roller til. *Periodisk revurdering – KMD Opus Debitor:* Økonomiforvaltningen har igangsat et rolle- og autorisationsprojekt, som skal understøtte funktionsadskillelse, herunder lukke konfliktende roller og implementere mitigerende kontroller. Projektet forventes afsluttet ultimo marts 2021.

Koncern IT
Strategi og
Forvaltningsrelationer
Borups Allé 177
2400 København NV

EAN-nummer
5798009809056

af brugere og tildelte rettigheder på tværs af systemer og forvaltninger. *Fratrædelser (KMD Aktiv):* I forbindelse med Deloittes stikprøvegennemgang af fratrædelser har de konstateret, at 2 brugere fortsat er aktive i KMD Aktiv efter deres fratrædelse *Oprettelser (Kvantum):* I forbindelse med Deloittes stikprøvegennemgang af tildelte udvidede rettigheder har de konstateret, at 1 af deres stikprøver ikke er udført på baggrund af en formel oprettelsesanmodning.		*Periodiske revurdering-KMD Opus Løn* Manglende procedure for periodisk gennemgang af tildelte rettigheder til brugere til OPUS løn løses med implementering af IGA-løsningen ved udgangen af Q1 2021. I forbindelse med ikke konsistent kontrol af funktionsadskillelse for OPUS løn er det indskærpet for teknisk systemejer, at denne skal varetages månedligt, jf. arbejdsgangen for systemet. *Periodisk revurdering – Kvantum:* Københavns Kommune er ved at implementere en IGA-løsning (ny adgangsstyringssystem for it), som vil løse denne bemærkning (de første test er afviklet). Økonomiforvaltningen forventer at afvikle periodiske revurderinger (ledelsestilsyn) ved udgangen af Q1 2021. Fratrædelser (KMD Aktiv): Der er fundet to brugere, der på revisionstidspunktet ikke var afsluttet. De to brugere er efterfølgende slettet i forbindelse med opfølgning på IGA-implementering. Punktet forventes at udgå ved næste revision. *Oprettelser (Kvantum):* Brugeren, der er oprettet uden om vanlig procedure, er oprettet ifm. et internt automatiseringsprojekt i Økonomiforvaltningen, hvor den pågældende udvikler er ansat. Økonomiforvaltningen (Koncern IT) vil gennemføre egenkontrol for de brugere, som

		oppebærer rettigheder, der muliggør oprettelse og nedlæggelse af brugere samt tildeling af rettigheder til brugere i Kvantum.

.

3.2.2 Revisionserklæringer	**Rettet mod: Økonomiforvaltningen**	**Omtalt år: 2017, 2018, 2019, 2020**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Deloitte har konstateret, at der er igangsat en proces til lukning af de oplistede bemærkninger i revisionserklæringerne. Der vil blive fulgt op på forholdene, når erklæringen for 2020 foreligger. Disse forventes primo 2021.	Deloitte henstiller, at der indhentes en specifik revisionserklæring for KMD Opus Debitor for at opnå en højere grad af sikkerhed. Endvidere vil Deloitte følge op på, at der indhentes relevant revisionserklæring vedr. Kvantum for 2020 til sikring af, at de konstaterede forhold i 2019 er lukkede.	*KMD Opus Debitor, KMD Opus Løn:* Der har løbende i 2020 været drøftelser mellem Økonomiforvaltningen og Deloitte om behovet for særskilt revisorerklæringer. Deloitte har efter interne drøftelser og i dialog med deres netværk besluttet, at der for deres kunder skal udarbejdes en særskilt erklæring. Dette krav vil som følge heraf indledningsvist møde de andre KMD Opus Debitor og KMD Opus Løn kommuner, og Københavns Kommune vil som led i handleplanen afsøge muligheden for at indgå i et (økonomisk) samarbejde om rekvirering af revisorerklæring på KMD Opus Debitor og KMD Opus Løn. *Kvantum* Økonomiforvaltningen (Koncernservice) forventer at modtage årlig revisorerklæring den 1. marts 2021. Åbenstående observationer fra revisorerklæring 2019 forventes lukket med undtagelse af to nedenstående forhold, som har en lukkedato efter 1. marts 2021. Det er p.t. 2 åbne observationer: 1.1) opdatering af database til seneste servicepack, som blev udskudt fra december til medio februar af hensyn til

		årsregnskabet 1.2) en patch opdatering af to Servere, som har afventet assistance fra SAP, planlagt gennemført i marts 2021. 2) Fællesbruger med privilegerede rettigheder (Sybase servere). KMD's driftsleverandør implementerer en generel løsning, kaldet PIM, i hele driftscentret for styring og dokumentation af fællesbrugere. Kvantum vil senest blive implementeret med udgangen af Q2 2021. Efter implementeringen vil KMD's revisor verificere, at dette forhold er bragt i orden.

3.2.4 BUF IT-drift (BIT)	**Rettet mod: Børn- og Ungeforvaltningen**	**Omtalt år: 2019, 2020**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Deloitte har konstateret, at der ikke er opsat tvunget periodisk skift af password for brugerne, som tilgår BIT's AD, baseret på KK's generelle krav til passwordpolitik. Det er dog oplyst, at der foreligger en handleplan til at få bragt området på plads således at det lever op til de generelle retningslinjer i KK. Det er endvidere oplyst, at BIT ikke har implementeret tvunget periodisk skifte af password endnu grundet COVID19. Efter det oplyste ligger handleplanen klar til godkendelse i Børn- og Ungeforvaltningen. På baggrund heraf opretholdes punktet.	Deloitte henstiller, at der arbejdes videre med implementeretingen af periodiske password skifte således at løsningen bliver underlagt det ønskede it-sikkerhedsniveau, som er fastlagt af Københavns Kommune.	Det tvungne passwordskifte var planlagt til forår 2020. Idet skolerne på det tidspunkt var ramt af nedlukning og hjemmeundervisning som følge af COVID 19, er tidsplanen blevet rykket. Børn- og Ungeforvaltningen forventer at flere brugere har behov for support til at skifte password. Skiftet skal derfor ske når skolerne er vendt tilbage til en normal hverdag. Det tvungne passwordskift må samtidig ikke placeres for tæt på skolernes afgangseksamen og for tæt på skolestart Tidsplan: Tidsplanen forudsætter at skolerne er tilbage til en normal hverdag efter sommerferien. - Februar 2021: Koordination med pilot-skoler og FAC - Marts 2021: Tidsplanen forelægges Børn- og Ungeforvaltningens direktion. - Forår 2021: Udarbejdelse af nødvendige

		vejledninger og kommunikation - September 2021: Tvunget passwords skifte implementeres på udvalgte pilot-skoler. - September 2021: Orientering i ugepakken om medarbejder passwordskifte - Oktober 2021: Samtlige medarbejdere på skoler afkræves passwordskifte - November 2021: Mulighed for implementering af passwordskifte for elever Når passwordskiftet først er opsat, vil lærere og pædagogiske medarbejdere én gang årligt blive afkrævet et password-skifte. I forbindelse med Aula-udrulningen på dagtilbud vil KK's pædagogiske medarbejdere på dagtilbud blive inkluderet i det pædagogiske AD og opsætte password i foråret 2021. Også de vil blive bedt om at ændre password året efter (altså forår 2022).

3.4.1 Kvantum – Standard profiler med udvidede rettigheder	**Rettet mod: Økonomiforvaltningen**	**Omtalt år: 2018, 2019, 2020**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Deloitte har i 2019 konstateret, at SAP standardbrugerne hos KMD for SAP* og DDIC ikke er blevet låst eller udløbet. Deloitte har i forbindelse med opfølgningen på sidste års observation konstateret, at de to brugere fortsat er aktive, men at de kun kan tilgås via secure server hos KMD. Deloitte har gennemgået loggen over anvendelsen og kan konstatere, at SAP* ikke har været anvendt i perioden samt at DDIC har været anvendt i forbindelse	Deloitte henstiller, at SAP* og DDIC låses for at reducere risikoen for misbrug.	Låsning af brugerne for SAP og DDIC er aftalt med KMD og procedurer og foranstaltninger for, hvordan disse i særlige nødstilfælde kan åbnes midlertidigt, er under udarbejdelse og vil være implementeret senest den 31. marts 2021.

med patchning i starten af revisionsperioden. Endvidere har Deloitte konstateret, at der pr. januar måned er lavet aftale med KMD om deaktivering af de to brugere. Samtidigt er der opsat en ny proces for aktivering og anvendelse af de to brugere hvor der kræves case by case review af anvendelsen. Deloitte vil efterteste denne proces i forbindelse med næste års revision. Baseret på den fremlagte proces forventer Deloitte at kunne lukke punktet i forbindelse med næste års revision.		

3.2.3 SharePoint	**Rettet mod: Børn- og Ungeforvaltningen**	**Omtalt år: 2020, 2021**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Deloitte har konstateret, at alle forvaltninger med undtagelse af Børn- og Ungeforvaltningen har færdiggjort oprydningsprojektet på SharePoint løsningen. Deloitte har dog konstateret, at Børn- og Ungeforvaltningen er den eneste forvaltning, som ikke har færdiggjort oprydningsprojektet, men at de efter oplyste forventer at være i mål Q1 2021. Det er dog forventningen, at Børn- og Ungeforvaltningen vil være færdige med rettighedsoprydning med udgangen af november 2020. Ud fra en risikovurdering har Børn- og Ungeforvaltningen valgt at fokusere på at begrænse rettigheder fremfor filsletning. På baggrund af, at der alene mangler færdiggørelse af	Deloitte henstiller, at oprydningsprojektet forsættes og gennemføres hos Børn- og Ungeforvaltningen efter planen.	Oprydningsprojektet i Børn- og Ungeforvaltningen består af: 1) Rettighedsoprydning (gennemført Q4 2020) og 2) Filoprydning (forventet gennemførsel Q2 2021). Oprydningsprojektet er pt. under gennemførsel med følgende status på delområder: 1. Rettighedsoprydning: Medlemskaber på samtlige afdelingssites er kontrolleret og evt. fejlrettet den 28/10. Alle skjulte mappebeskyttelser er fjernet fra alle sites i november 2020, hvorefter der er overensstemmelse mellem filer og dem, der har adgang til at se filerne. Oprydning af medlemskaber nu afsluttet med undtagelse af følgende, som har været uden for scope: a. Ledersites oprettet ifm. oprydning til håndtering af

oprydningsprojektet i Børn- og Ungeforvaltningen nedprioriteres punktet og Deloitte forventer, at denne kan lukkes i forbindelse med revisionen 2021.		filer med særlig adgangsbegrænsning. b. Projektsites oprettet efter migreringen, hvorfor der ikke optræder forældede rettigheder fra de tidligere netværksdrev. Site med højt medlemsantal håndteres manuelt i Q1 2021. Øvrige sites indgår i rettighedsvedligehold med implementering af rapporter fra KIT til site- og data-ejere (forventet februar 2021). c. Enkelte sites, hvor oprydningen skal håndteres manuelt pga. teknisk fejl. Oprydning håndteres manuelt Q1 2021. 2. Filoprydning: Sideløbende med rettighedsoprydning er der i 2020 igangsat manuel oprydning af følsomme filer med anbefaling til fremgangsmåde samt med mulighed for support. Opgaven har deadline 31. marts 2021 med opfølgning og kontrol af resultat den 1. april 2021. a. Der gennemføres delkontrol af fremgang i opgaven januar 2021. Ved evt. manglende fremgang gennemføres følgende februar 2021: i. Orientering til områdeledelsen med anmodning om øget opmærksomheden på opgaven. ii. Direkte kontakt til siteejerne, hvor der er størst risiko (mange filer kombineret med mange medlemmer). b. Kontrol 1. april danner afsæt for at vurdere nødvendigheden af udmelding omkring automatisk sletning pr. 1. juni 2021. Projektet afsluttes dermed senest Q2 2021.