Bilag 2 – Handleplaner generelle it-kontroller 2019

3.1.1 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 databeskyttelsesfor-ordningens 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.	Det er i O365-styregruppen aftalt, at forvaltningerne senest 1. januar 2020 skal have udarbejdet forvaltningsspecifikke tidsplaner for oprydning af filer og rettigheder i SharePoint. Det følger af den forvaltningsspecifikke it-revision, at alle forvaltninger skal have gennemført oprydning af filer og rettigheder i SharePoint med udgangen 1. kvartal 2020. KIT vil afrapportere til It-kredsen om status på forvaltningernes oprydning primo februar og primo april 2020. **Beskæftigelses- og Integrationsforvaltningen** Beskæftigelses og integrationsforvaltningen direktionsbehandler oprydningsprojektet medio januar 2020. Forvaltningen forventer at have gennemført oprydningsprojektet inden 1.5.2020. **Børne- og Ungdomsforvaltningen** BUF har igangsat arbejdet og starter med at fjerne adgange for de allermest kritiske sites. I december 19 gennemføres en pilot i Digitalisering og Data. Primo januar drøftes den videre oprydning med områdeledelsen med henblik på at få tilrettelagt oprydningen decentralt. Det bliver en meget omfattende opgave for BUFs decentrale ledere. Derfor er BUF i lighed med de øvrige forvaltninger bekymret for tidsperspektivet og kommer til at gennemføre oprydningen på baggrund af en risikobaseret tilgang der sikrer hensynet til kernedriften. Sites med meget store medlemsantal behandles først. Sideløbende som mitigerende handling, oprettes særskilte sites til ledere i BUF, hvor evt. beskyttede ledelsesmapper kan flyttes forud for sletning af rettigheder på samtlige sites. Ved nærmere fastlagt dato (forventet januar/februar 2020), slettes alle

Bilag 2 – Handleplaner generelle it-kontroller 2019

		gruppemedlemmer og nedbrudte rettigheder, med efterfølgende genindskrivning af rette gruppemedlemmer efter enhedens KK-org. Sideløbende slettes sites, der ikke længere er aktive. Sletning af filer følger derefter i særskilt forløb: Fase 1 i Q1 2020: Kommunikationsmateriale under rettighedsoprydning indeholder tilskyndelse til at igangsætte oprydning af filer. Henvisning til kommende rolle som dataansvarlig og siteejer. Fase 2 i Q1 og Q2 2020: Sletning af filer udføres. Evt. indmelding af "fredning" af filer i ark. Behov for accept af automatisk sletning pba. tidligere indmeldte principper (fx alder, aktivitet, filtype). Fase 3 i 2020 efter gennemført sletning i Q2: Kontrol af resultatet – identificering og håndtering af sites med fortsat store antal filer? **Kultur- og Fritidsforvaltningen handleplan** Oprydningsprojektet fortsætter i KFF efter særskilt plan jf. nedenfor: Overordnet vedrører indsatsen at fjerne adgange, og flytte filer til afgrænsede arbejdsfællesskaber, således at medarbejdere kun har adgang til de filer, som er indenfor medarbejderens eget arbejdsområde. *Status pr 20. december:* Gennemført fase 0, som omfatter fjernelse af adgangsrettigheder og brudte rettigheder til over 50 % af alle KFF sites (1079 til 500). Derudover er der fjernet adgang til alle sites med mere end 250 medlemmer. *Næste deadline 30 april.* Næste fase løber frem til 30 april 2020 og indbefatter resterende sites herunder løbende oprydning i alle filer og rettigheder, og etablering af ny gruppebaseret struktur, der afspejler de faktiske arbejdsfællesskaber.

Bilag 2 – Handleplaner generelle it-kontroller 2019

		Teknik- og Miljøforvaltningen handleplan Teknik- og Miljøforvaltningen foretager oprydning via en struktureret og risikobaseret tilgang. På ca. 20 pct. af forvaltningens sites (tidligere fællesdrev), som vurderes at være de mest kritiske, er der inden udgangen af 2019 gennemført adgangsbegrænsning samt reduktion af unikke rettigheder på mappe- og filniveau. Der gennemføres i løbet af 1. kvartal 2020 oprydning på de resterende sites. Rettigheder fjernes på passive sites, som lægges i arkiv ved udgangen af januar 2020 med forventet endelig sletning af sites, der ikke er reaktiveret, efter tre måneder. Processen skal sikre, at relevant data, som anvendes i forvaltningen, ikke slettes. Herudover gennemføres en automatiseret sletning af inaktive filer, og de ansvarlige for de forskellige sites skal forholde sig til rettigheder og manuel sletning ud fra fastlagte principper. **Socialforvaltningen handleplan:** *Rettigheder:* SOF har pr. d. 12/12/19 fuldt gennemført oprydning og sletning af rettigheder i vores Sharepoint-sites. Efter oprydningen er antallet af aktive sites faldet fra 2843 til ca. 400. *Oprydning i filer:* I november og december er der gennemført en pilot i Digitaliseringsenheden for at indsamle viden til den øvrige forvaltnings oprydning. Oprydningen forventes gennemført pr. 1 juli 2020. For at kunne påbegynde arbejdet med oprydningen i filerne på de aktive sites, har SOF brug for automatiseret og datamæssig understøttelse til processen via KITs governancemotor da det drejer sig om mere end 2,5 mio. filer. SOF har efterspurgt understøttelsen siden

		starten af året, men det er fortsat uklart, hvornår motoren stilles til rådighed således, at opgaven de enkelte ledere og afdelinger står overfor bliver realistisk at gennemføre. Governancemotoren er endvidere kritisk i forhold til at give SOFs ledere overblik til egenkontrol og ledelsestilsyn. For ressourcemæssigt at kunne gennemføre oprydninger er opgaven opdelt pr. borgercenter. Tidsplanen i SOF er følgende: 1. Pilot i november/december 2019 2. Oprydning hos centrale kontorer januar/februar 2020 3. Oprydning hos Borgercenter Voksne februar/marts 2020 4. Oprydning hos Borgercenter Handicap februar/marts 2020 5. Oprydning Borgercenter Hjemmepleje april/maj 2020 6. Oprydning Borgercenter Børn og Unge i maj/juni 2020 **Sundheds- og Omsorgsforvaltningen** SUF foretager oprydningen ud fra en risikobaseret tilgang, hvor SharePoint-sider med 700+ medlemmer håndteres først. Dette tæller blandt andet en række tidligere områdedrev, der løbende lukkes i januar 2020. SUF's øvrige enheder (plejehjem, hjemmeplejen, bydækkende enheder mm.) håndbæres således, at oprydningen og den fremtidige brug af SharePoint sker ud fra en række overordnede principper i SUF, der har til formål at kvalificere oprydningen og understøtte den fremtidige brug af platformen. Dette forventes tilendebragt maj 2020. Det er dog afgørende, at den aftalte selfservice-løsning af Office 365-grupper, som forvaltningerne forventede i indeværende år, gøres tilgængelig. Ligeledes er det afhørende, at Microsofts Teams gøres tilgængelig. En fortsat udeblivelse af disse vil betyde, at deadline vil rykke sig yderligere. Nedenstående tidsplan blev fremsendt til KIT før jul i forbindelse med ITK. Oprydning i rettigheder: Deadline for oprydning i rettigheder

Bilag 2 – Handleplaner generelle it-kontroller 2019

		Status: er i gang SharePoint-sites med 700+ medlemmer: Januar 2020 Øvrige SharePoint-sites: Maj 2020 **Økonomiforvaltningen** ØKF har gennemført fjernelse af alle rettigheder på alle sites, og efterfølgende tildelt rettigheder på ny. Dokumenter er blevet gennemgået, og det er vurderet, hvilke sites og filer, som skal flyttes til arkiv og efterfølgende slettes.

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.1.2 Pædagogisk it (PIT) ●	Rettet mod: Økonomiforvaltningen	Omtalt år: 2019
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Pædagogisk IT Vi har konstateret, PIT benytter Azure Active Directory, hvor samtlige elever, lærere og andet personale på skolerne står registreret med deres UNI-Login. Det er oplyst, at PIT's AD er totalt adskilt fra KIT's AD. Yderligere er det oplyst, at grundet tekniske begrænsninger er det ikke muligt at gennemtvinge KK's krav til password på PIT's AD. **Risici** En 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 på en løsning således at PIT bliver underlagt det ønskede it-sikkerhedsniveau fastlagt af KIT.	BUF har allerede igangsat flere tiltag for at være klar til når STIL d. 18/2-2019 lancere den nye UNI-login og dermed samtidig stopper password synkroniserings-servicen. Som nævnt vil BUFs elever og pædagogiske medarbejdere fremover anvende PIT Azure AD til login til AULA, læringsplatforme, digitale læremidler ved at anvende STIL's føderationsløsning. BUF forvaltningens handleplaner består af 3 spor: **1. Spor: Teknisk implementering – Januar/Februar 2020** PIT foretager de nødvendige tekniske konfigurationer af PITs Azure AD med regler og policies, så det opfylder password-politikker baseret på KK's krav, såsom krav til antal tegn, kompleksiteten samt hvor ofte det skal skiftes. **2. Spor: Udvikling af værktøj til decentral password-reset – Januar 2020** Hidtil har de ansvarlige på skolerne kunne logge på brugeradministration.emu.dk og nulstille password hvis elever eller pædagogiske medarbejdere havde glemt deres password. Pædagogisk IT er i gang med at få udviklet en webservice, hvor kun de medarbejdere der har fået tildelt rettigheder til at nulstille password, kan fremsøge deres elever og nulstille deres password. De pædagogiske medarbejdere vil kunne anvende Microsofts eget selfservice (Jeg har glemt mig adgangskode) til at nulstille deres password. De pædagogiske medarbejdere vil også være muligt at kontakte PITs Serivicedesk og få hjælp til at få nulstillet deres password. **3. Spor: Information og kommunikation – Januar 2020**

Bilag 2 – Handleplaner generelle it-kontroller 2019

		BUF udarbejder de nødvendige vejledninger (PDF og evt. videoguides) og informere deres brugere i forhold til de kommende ændringer på området.

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.2.1 Styring af brugerrettigheder og systemadgange ●	Rettet mod: Forvaltningerne	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 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.	**Opus Debitor - funktionsadskillelse** Roller og autorisationer i OPUS debitor kortlægges med henblik på sikring af funktionsadskillelse. Dette gøres ved: - Kortlægning af standardroller i OPUS med KMD - Kortlægning af andre kommuners brug af roller - Roller og risici i Opus Debitor afdækkes mod KMD standardroller De identificerede risici håndteres ved følgende aktiviteter: - Involvering af forvaltningerne for at understøtte fremtidigt behov - Lukning af kritiske adgange og/eller etablere mitigerende kontroller - Udarbejdelse af rollematrix, der sikrer funktionsadskillelse Deadline 31-03-2020 **Opus Debitor - Periodisk revurdering** *Periodisk revurdering* Koncept for opfølgning på autorisationer i forbindelse med periodisk revurdering og håndtering af fratrædelser udarbejdes med henblik på fastholdelse af relevante roller og lukning af autorisationer, som ikke længere skal være gældende. Deadline 31-12-2019 **Kvantum - periodisk revurdering** *Periodisk revurdering* Governance for periodisk revurdering er beskrevet og kommunikeret til Budget- og Regnskabskredsen i juli måned af KS og KIT. Den valgte governance for ledelsestilsyn, som er besluttet i Økonomiudvalget beskrevet i forretningscirkulæret for ledelsestilsyn anfører, at KS skal fremsende materiale, således at forvaltningerne kan foretage det besluttede

Bilag 2 – Handleplaner generelle it-kontroller 2019

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 at 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 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.		ledelsestilsyn. Dermed er det forvaltningernes ansvar at følge op på, at der decentralt er gennemført ledelsestilsyn. Deadline: 31-08-2019 (gennemført) **Håndtering af fratrædelser i Opus Debitor, Kvantum, KMD Aktiv** Der implementeres indledningsvist en semiautomatisk løsning, der medfører, at der ifm. fratrædelse/flyt automatisk genereres en opgave i ServiceNow til BA om, at den pågældende medarbejder fratræder/flytter pr. dato xx, og derfor skal have lukket sin adgang(-e) til Kvantum,/ Opus Debitor / KMD Aktiv, såfremt medarbejderen har sådanne. Deadline: 31-01-2020 På længere sigt erstattes denne løsning med en fuldautomatisk løsning i regi af IGA, hvor lukning af adgange sker automatisk via en integration fra ServiceNow til IGA-løsningen. Implementeringen af IGA-løsningen forventes endeligt afsluttet i september 2021, hvorfor der indtil da vil blive tale om paralleldrift med henblik på at sikre rettidig og korrekt fjernelse af brugerrettigheder ved interne flytninger og fratrædelser. Deadline: 4. Kvartal 2021 **KMD Aktiv – Beskæftigelses- og Integrationsforvaltningen** 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. BA vil igen blive henstillet at følge gældende retningslinjer for tildeling og nedlæggelse af brugere i KMD Aktiv.

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.2.2 Revisionserklæringer ●	Rettet mod: Forvaltningerne	Omtalt år: 2017, 2018 og 2019
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
Københavns Kommune har indgået aftale med KMD omkring drift af Kvantum, KMD Aktiv og KMD Debitor 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 KMD Kvantum og KMD Aktiv. Det er oplyst, at det er aftalt med KMD, at systemrevisionserklæring for Kvantum skal foreligge senest 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 ikke bekendt med. **Status 2019** Vi har konstateret, at der 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. **Risici** 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.	**KMD Debitor** Henset til at OPUS Debitor er en fælles løsning for ca. 70 kommuner, vil KK afsøge mulighederne for, at der hos KMD indhentes en fælles, systemspecifik KMD Opus Debitor revisorerklæring, der er gældende for samtlige kommuner, hvorved omkostningerne pr. kommune og dermed for KK reduceres. Deadline afhænger af, hvorvidt KMD er i stand til at levere indenfor den angivne tidshorisont. Deadline: 29-02-2020 **KMD Aktiv – Beskæftigelses- og Integrationsforvaltningen** Revisorerkæring rekvireres hvert år i marts/april måned fra leverandøren.

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.4.1 Kvantum – standardprofiler med udvidede rettigheder	**Rettet mod: Økonomiforvaltningen**	**Omtalt år: 2018 og 2019**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
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 SAP* og DDIC ikke er blevet låst eller udløbet. **Risici** 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.	**SAP* og DDIC** Der er implementeret en løsning, så SAP* og DDIC kun anvendes af KMD, og kun i de tilfælde hvor udviklere fra KMD har behov for at tilgå produktionsmiljøet. Løsningen indebærer at al brug af SAP* og DDIC sker via Secure Server og al aktivitet logges. Deadline: 31-12-2019

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.4.2 Kvantum – change management test	Rettet mod: Økonomiforvaltningen	Omtalt år: 2018 og 2019
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
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 test dokumentation for 7 ud af 25 ændringer ikke kunne leveres. De 7 ændringer var idriftsat før 1. april 2019. Vi nedprioriterer punktet og forventer at denne kan lukkes i forbindelse med revisionen 2020. **Risici** 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 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.	**Kvantum - Change management - Test** Der er pr. 1. april 2019 implementeret governance for sikring af kvalitet og dokumentation af test gældende for alle ændringer i Kvantum. Dokumentation for gennemført test opbevares i ServiceNow. Deadline: 01-04-2019

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.4.3 Governance-modellen for anvendelse af SIEM	**Rettet mod: Økonomiforvaltningen**	**Omtalt år: 2018 og 2019**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
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 uddannelsesprogram forventes	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 informationsmanagement-systemet (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.	Koncern IT vil i Q1 2020 og Q2 2020 afholde specifikke workshops om risiko-awareness og ISO 27001 for de syv forvaltninger, som en del af et ’kick off’ for den nye og forbedrede obligatoriske systemejeruddannelse. Ud fra en risikovurderet tilgang vil deltagerne være udvalgte forretningsmæssige- og tekniske systemejere for systemer, der er vurderet forretningskritiske for KK.

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 har i 2019 udarbejdet og formidlet revideret materiale og vejledning om logning og logopfølgning til forvaltningerne. **Risici** 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.		

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.4.4 Governance-modellen for udvikling og drift af robotter/automatisering af processer	**Rettet mod: Økonomiforvaltningen**	**Omtalt år: 2018 og 2019**
Observationer og risici	**Revisionsbemærkning**	**Handleplan**
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 2 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.	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). Vi anbefaler at der laves en gennemgang af tidligere implementerede robotter for at sikre, at disse er underlagt governance modellen	ØKF vil i Q1 2020 gennemgå alle nuværende idriftsatte RPA-løsninger i forvaltningerne for konformitet med RPA-governancemodellen. De steder hvor der konstateres mangler, vil ØKF/KIT indstille overfor forvaltningerne, at forretningsejerne i dialog med ØKF/KIT sikrer konformitet, alternativt at de ikke-konforme robotter afvikles.

Bilag 2 – Handleplaner generelle it-kontroller 2019

3.4.5 It-sikkerhedsvurderinger	**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 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.	For 2019 udestår, at forvaltninger får lukket de af KIT fremsatte henstillinger vedrørende risikovurderingerne for 2018.	Det fremgår af konceptet for risikovurderinger, at det er obligatorisk for alle forvaltninger at lukke eventuelle henstillinger. I forlængelse heraf skal alle forvaltninger med udgangen af 2019 dokumentere, at de har lukket alle henstillinger fra risikovurdering 2018. ØKF/KIT indmelder en endelig status på it-kredsmødet d. 20. december 2019 på forvaltningernes håndtering af henstillinger fra risikovurdering 2018. For så vidt angår opfølgningen på risikovurderinger for 2019 i 2010 har KIT meddelt alle forvaltninger, at opfølgning vil foregå efter denne plan: Marts 2020 Forvaltningen behandler risikovurderingen for 2019 og udarbejder handleplaner for systemerne. Den direktionsgodkendte handleplan fremsendes til KIT. April 2020 KIT udarbejder en samlet opfølgning til DCK og It-kredsen, som tager afsæt i forvaltningernes handlingsplaner. September 2020 Forvaltningen fremsender opfølgning og status på handleplanen til KIT, der orienterer DCK og It-kredsen November/december 2020 Forvaltningen fremsender opfølgning og status på handleplanen til KIT, der orienterer DCK og It-kredsen **Beskæftigelses- og Integrationsforvaltningens 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. **Socialforvaltningen handleplan** Opfølgning på henstillinger fra KIT til SOFs handleplan for risikovurderingerne i 2018. **Spydspidsen:**

Bilag 2 – Handleplaner generelle it-kontroller 2019

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.

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.

1. Der er indgået en databehandler-aftale med EG. Da systemet er er opsagt og man er i gang med udfasning og der er ikke iværksat yderligere foranstaltninger

Brugerjournalen:
Systemet er opsagt pr. 31.12.2019 og brugerne er overgået til at arbejde i Novax i efteråret 2019.12.20

KMD Erindring:
KIT drifter systemet og der er tale om interne data, hvor for der ikke er behov for en databehandleraftale. Det undersøges fortsat om systemet kan udfases.

BAS:
Driftschefen har i nov. 2019 været i dialog med systemejeren på BAS. Det viser sig, at man fejlagtigt, har anført, at man ikke kunne berigtige data – det kan man GODT i BAS. Dette er nu rettet i risikovurderings-skemaet

Sundheds- og Omsorgsforvaltningens handleplan
KIT foretog i ultimo 2018 en risikovurdering af 10 udvalgt it-systemer i SUF. Opfølgning på handleplaner blev sendt til KIT – Vejledende Sikkerhed 4. dec. 2019. Hermed handleplan for henstillingerne, der endnu ikke er implementeret.

Henstillinger der ikke er implementeret **Systemnavn**	**Henstilling der ikke er implementeret**	**Handleplan**	
Cura	ID:D1 Slettefrister ID:D3 Berigtigelse	Begge opgaver er under implementering, men pga. opgavernes størrelse er de ikke gennemført i 2019. Konkrete slettefrister er fastsat, selve implementeringen er undervejs. Der kan ikke gives konkret tidshorisont på nuværende tidspunkt.	
SUF Kasser	ID:C3	Databehandleraftale forventes indgået i	

Bilag 2 – Handleplaner generelle it-kontroller 2019

			Indgåelse af fornødne databehandleraftaler	løbet af januar 2020	