3.1.1 - Styring af brugerrettigheder og systemadgange	Ansvarlige: Vibeke Nymann (Kvantum) Pia Ilsø (KMD Opus) Freddy Lassen (eDoc) Anders Reuter (Brugeradministrationen)	Deadline: 31. marts 2019/Gennemført

Observationer og risici	Risikobeskrivelse	Anbefaling	Revisionsopfølgning 🔴
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/adgangsrettigheder, 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 brugeradministrationsproceduren følges, således at tildeling af rettigheder til brugere sker på baggrund af formelle og dokumenterede autorisationer	Økonomiforvaltningen er enig i revisions-bemærkningen vedrørende styring af brugerrettigheder og systemadgange. Handlingsplanen er generisk for Kvantum og KMD Opus, dog med den forskel, at KMD Opus har en mere snæver brugerkreds og er et fælleskommunalt system fra KMD, som kommunen lejer sig ind på. Tildeling af rettigheder Bemærkningen er målrettet KMD Aktiv Periodisk revurdering (overvågning) • KS designer og implementerer forretnings-regler for periodisk tilbagevendende lukning af inaktive brugere som Brugeradministrationen efterfølgende lukker. • KS har udarbejdet en vejledning til dataudtræk som den stedlige ledelse i kommunens enheder skal basere det årlige ledelsestilsyn på. Derudover vil KS supportere spørgsmål i den forbindelse. • KS foretager en årlig SOD analyse med henblik på at afdække risici ved manglende funktionsadskillelse som følge af tildelte adgangsrettigheder. Eventuelle SOD konflikter der identificeres i den forbindelse mitigeres ved enten organisatorisk funktionsadskillelse og/eller design og implementering af mitigerende kontroller. • KIT foretager hvert år et udtræk over de adgange som findes i eDoc. Udtrækket fremsendes til forvaltningerne, som sikrer sig at brugerne har de korrekte rettigheder. Denne proces sikrer, at det er de dataansvarlige som holder tilsyn med hvem der har adgang til deres data. En varig løsning på periodisk revurdering er at anskaffe

			og implementere et SAP værktøj, som systemmæssigt sikrer automatisk, præventiv kontrol af funktionsadskillelse i forbindelse med tildeling af rettigheder. Herved vil en årlig SOD analyse kunne overflødiggøres, ligesom det decentrale ledelsestilsyn vil kunne reduceres betragteligt. KS er i gang med at udarbejde investeringscase herpå. Fratrædelser (nedlæggelser) • KS designer og implementerer proces som Brugeradministrationen efterfølgende drifter i henhold til. Ovenstående er designet og implementeret: Kvantum: 31.3.2019. Opus Debitor: 30.6.2019 Fsv. angår anbefalingen tildelingen af rettigheder, kan KIT oplyse at den centrale brugerstyring i dag foregår efter formelle og dokumenterede autorisationsprocedurer, hvor bestilling af autorisationer sker ved, at den relevante autorisationsansvarlige bestiller adgange via det centrale sagsstyringssystem. Den manglende dokumentation for de 4 ud af 25 udvalgte stikprøver foreligger i arkiv, idet de tilhørende oprettelser i KMD Aktiv er sket i et tidligere, nu udfaset, sagsstyringssystem.

3.1.2 Kvantum – Standard profiler med udvidede rettigheder	Ansvarlige: Vibeke Nymann	Deadline: Gennemført	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning** 🔴
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	Økonomiforvaltningen er enig i revisions-bemærkningen vedrørende standard profiler med udvidede rettigheder. **SAP_ALL på KP0, KP5, KP6 og KPA rettigheder** Der er fulgt op på dette forhold, og der er ikke længere nogen KK brugere med disse rettigheder. **SAP* og DDIC** KMD har etableret en procedure for anvendelsen af SAP* og DDIC således, at de kun kan bruges som tiltænkt, det vil sige, at de dokumenteres på KMD secure server, og kun anvendes ved behov for nødbrugeradgang, når alt andet går galt.

3.1.3 Kvantum – Change management - Test	Ansvarlige: Vibeke Nymann	Deadline: 1. april 2019	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning** 🔴
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.	Økonomiforvaltningen er enig i revisions-bemærkningen vedrørende dokumentation af test af ændringer i visse tilfælde er mangelfuldt. **Handlingsplan** KS er i gang med at implementere en version 1 proces for test af ændringer, der implementeres i Kvantum. Denne vil være implementeret pr. 1.4.2019. I takt med at der implementeres egentlig releasestyring vil testprocessen blive yderligere forfinet, hvilket forventes i 4. kvartal 2019.

3.2.1 It-sikkerhedsvurderinger	Ansvarlige: Frederik Siegumfeldt	Deadline: Q2 2019

Observationer og risici	Risikobeskrivelse	Anbefaling	Revisionsopfølgning
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.	**KIT - Handleplan** Fsv. angår anbefaling nr. 1 er forholdet efter revisionens gennemførelse håndteret af KK, hvilket Deloitte har anerkendt i rapporten. Dette gør sig også gældende for den del af anbefaling nr. 2 vedr. 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. Fsv. angår anbefaling vedr. forvaltningsdirektionens godkendelse af risikoappetitten og risikohåndteringsplanen, har Økonomiforvaltningen i risikorapporter af 21. december 2018 henstillet, at forvaltningernes ledelser kvalificerer risikoen for forvaltningens varetagelse af opgaver inden for de udvalgte fagområder, og at forvaltningerne på baggrund af risikoappetitten iværksætter yderligere sikringsforanstaltninger. **Forvaltningernes handleplaner** **Økonomiforvaltningen** ØKF's koncerndirektion har på møde den 4. februar 2019 taget stilling til den videre håndtering af systemrisici og eventuelle yderligere foranstaltninger. Økonomiforvaltningen (Koncern IT) vil i løbet af Q2 2019 anmode om en tilbagemelding fra de øvrige forvaltninger ift. deres håndtering af systemrisici og eventuelle yderligere foranstaltninger. **Beskæftigelses- og Integrationsforvaltningen** BIF har igangsat den af KIT påkrævede opdaterede risikovurdering af BIF´s kritiske systemer. Risikovurderingen foretages ud fra KITs standard til området og vil ud over vurderingen også indeholde handleplan for de nødvendige tiltag. Risikovurderingen og handleplanen direktionsbehandles i BIF primo Q2. **Børne- og Ungdomsforvaltningen** BUF gennemførte i 2017 risikovurderinger på i alt 9 forretningskritiske systemer. BUFs direktion godkendte handleplanen d. 18.12 2017.

			I efteråret 2018 har BUF tilsvarende gennemført risikovurdering af 7 forretningskritiske systemer, som fremlægges tilsvarende for BUFs direktion mhp. godkendelse af risici og indsatser i april 2019. Pt. afventer BUF en gennemgang med Økonomiforvaltningen ift. afrapporteringen, der gennemføres i marts 2019. **Kultur- og Fritidsforvaltningen** Center for Digitalisering og Innovation er ved at planlægge en gennemgang af risikovurderingen med deltagelse af relevante system- og procesejere med henblik på forelæggelse for KFFs direktion. Gennemgangen vil omfatte en vurdering af den manglende sikringsforanstaltning ift. relevans, risiko, tilgængelighed, forretningskonsekvenser samt vurdering af omfanget af imødegående handlinger. Gennemgangen skal gøre direktionen i stand til at træffe beslutning ift. risikoappetit og -håndtering på områderne. **Socialforvaltningen** SOF har foretaget den af KIT påkrævede opdaterede risikovurdering af SOFs kritiske systemer i slutningen af 2018. Risikovurderingen er foretaget ud fra KITs standard til området og inkluderer ud over vurderingen også en handleplan for de nødvendige tiltag. Risikovurderingen og handleplanen er direktionsgodkendt i SOF den 30. januar 2019. Ud over arbejdet med risikovurderinger af SOFs kritiske systemer har SOF også aktivt bidraget til KITs genetableringsplan, der ser på risici på tværs af it-systemerne. **Sundheds- og Omsorgsforvaltningen** SUF gennemførte ultimo 2017 risikovurderinger på alle systemer forvaltningen er ansvarlig for. SUFs direktion godkendte 13. december 2017 risikovurdering og indsatser. Økonomiforvaltningens risikorapporter af 21. december 2018 fremlægges tilsvarende for SUFs direktion mhp. godkendelse af risici og indsatser. **Teknik- og Miljøforvaltningen** TMF har fået risikovurderet 10 systemer og alle vurderinger er komme ud med risici der ligger på middel eller lav. I starten af februar holdt TMF møde med KIT IT-Sikkerhed for at få planlagt det videre arbejdede med KIT IT-Sikkerhed anbefalinger.

			TMF Stab Digitalisering er i gang med at holde møder med systemejerne for de 10 risikovurderede systemer, på møderne gennemgås rapportens findings, hvorefter der tages stilling til hvilke aktiviteter der skal igangsættes, i forhold til at følge anbefalingerne fra KIT IT-Sikkerhed. Alle beslutninger vil blive dokumenteret i den skabelon som TMF har fået stillet til rådighed fra KIT IT-Sikkerhed, når dette arbejde er afsluttet, vil resultatet blive forelagt TMF's direktion.

3.2.2 Beredskabsplaner	Ansvarlige: Frederik Siegumfeldt	Deadline: 1.4.2019	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning**
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.	**KIT - Handleplan** Den tværgående Plan for fortsat it-drift i Københavns Kommune og Strategisk plan for it-genopretning blev godkendt på It-kredsens møde den 21. december 2018. Det blev på samme møde besluttet, at de enkelte forvaltningers it-beredskabsplaner forventes at være udarbejdet og ledelsesgodkendt senest 1. april 2019. Det fremgår af Plan for fortsat it-drift i Københavns Kommune, at planen revideres en gang om året eller ved væsentlige ændringer i de faktiske forhold med betydning for planen **Forvaltningernes handleplaner** **Økonomiforvaltningen** Kernen i ØKF's individuelle beredskabsplan består af systemspecifikke nødplaner, hvori der skal tages stilling til håndteringen af forretningskritiske arbejdsopgaver i tilfælde af it-nedbrud. Nødplanerne skal udfyldes af de enkelte koncernenheder (de forretningsansvarlige). Skabelon for nødplaner er udarbejdet og er drøftet med koncernenhederne på et møde den 31. januar 2019. Intern ØKF-frist for udarbejdelse af nødplaner er den 8. marts 2019, hvorefter KIT forelægger en samlet ØKF-beredskabsplan til godkendelse i Økonomiforvaltningens direktion. **Beskæftigelses- og Integrationsforvaltningen** BIF har udarbejdet it-beredskabsplaner for de forretningskritiske systemer og senest lavet opfølgning i januar 2019. Reviderede beredskabsplaner vil blive forlagt direktionen primo Q2. **Børne- og Ungdomsforvaltningen** BUF er i gang med at udarbejde de udestående, konkrete forvaltningsspecifikke it-beredskabsplaner med udgangspunkt i beslutningen den 21. december 2018. BUF arbejder målrettet mod at færdiggøre handleplanerne som forudsat 1. april 2019. Der kan dog være behov for, at processen omkring bl.a.

			ledelsesforankring sker efterfølgende af hensyn til kvaliteten af handleplanerne. **Kultur- og Fritidsforvaltningen** KFF har udarbejdet udkast til "Beredskabsplan for it understøttede processer for KFF", der med udgangspunkt i de 4 mest kritiske systemer i forvaltningen redegør for, hvem, der gør hvad i en beredskabssituation. Beredskabsplanen forventes godkendt i KFFs direktion inden udgangen af marts 2019. Der forventes gennemført en beredskabsøvelse i Q2, hvor beredskabsplanen vil blive testet. **Socialforvaltningen** SOF har i 2018 udarbejdet en opdateret IT-beredskabsplan. Planen er behandlet og direktionsgodkendt i SOF d. 05. maj 2018. **Sundheds- og Omsorgsforvaltningen** SUFs overordnede forvaltningsspecifikke it-beredskabsplan blev godkendt af SUFs direktions 2. maj 2018. I Økonomiforvaltningens risikorapport af 21. december 2018 af 11 særligt udvalgte SUF-systemer fremgår at der er systemberedskabsplan for kritikalitet 1 og 2-systemer samt for alle undtagen 2 kritikalitet 3-systemer. ØKF anbefaler at SUF overvejer om der er behov for beredskabsplaner på de to systemer. SUF er pt. i gang med at afklare behovet. **Teknik- og Miljøforvaltningen** Af de 20 It-systemer der anses som kritiske for TMF er der udarbejdet beredskabsplaner for de 15 It-systemer. Der er planlagt et forløb som skal sikre, at der er udarbejdet beredskabsplaner for de sidste 5 kritiske It-systemer inden 19 april 2019. TMF's direktion vil blive orienteret om status på TMF's beredskabsplaner i Q2 2019.

3.2.3 Revisionserklæringer	Ansvarlige:	Deadline: 1.4.2019	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning**
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.	KS har bestilt en udvidet revisor erklæring hos KMD vedr. Kvantum. KK afventer en konkret dato for, hvornår denne kan forventes leveret af KMD. Forventet deadline: 1.4.2019

3.4.1 Governance-modellen for anvendelse af SIEM	Ansvarlige: Anders Reuter & Freddy Lassen	Deadline: Q3 2019	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning**
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.	Workshop gennemføres i tæt samarbejde med DCK, hvor KIT sikrer koordinering af indhold, deltagere mv. Workshop gennemføres i tæt samarbejde med DCK, hvor KIT sikrer koordinering af indhold, deltagere mv. KIT inviterer relevante deltagere fra alle forvaltninger til et præsentationsarrangement. Dokumentation og retningslinjer revurderes og publiceres.

3.4.2 Governance-modellen for udvikling og drift af robotter / automatiserede processer	Ansvarlige: Jacob Honoré	Deadline: Gennemført/ultimo 2019	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning**

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-sikkerhedsniveau 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).	Kontrol af adgange til UiPath vil fremover indgå som et led i det årlige ledelsestilsyn på autorisationer og adgange. Adgange er herudover ændret til at være styret igennem AD. Planlægges at være klar ultimo 2019 Ved idriftsættelsen af alle robotter foretages der et såkaldt 'codereview', hvor koden og dokumentationen gennemgås og godkendes. Fremover vil testhandlinger indgå som et obligatorisk led i at få et godkendt 'codereview'. Alle driftsaftaler fra 2019 og fremover vil indeholde en uddybning af ansvarsfordelingen i overvågningen af input/output af robotterne. Driftsaftaler lavet før 2019 vil blive opdateret med denne uddybning.

3.4.3 It-risikoanalyse - Kvantum	**Ansvarlige:**	**Deadline: 1.4.2019**	
Observationer og risici	**Risikobeskrivelse**	**Anbefaling**	**Revisionsopfølgning** 🟡
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.	Mht. den tidligere gennemførte sikkerhedsvurdering for Kvantum, er KK i gang med at vurdere behovet for kryptering og derefter sikre, at den relevante forvaltningsgodkendelse foretages. Forventet deadline: 1.4.2019