Bilag 2 - Handleplaner til Revision af generelle IT-kontroller

Revision af generelle IT-kontroller	
3.1.1 Tildeling af autorisationer (Kvantum) (rød)	Økonomiforvaltningen
3.1.2 Adgang til at administrere batchjobs (Kvantum) (rød)	Økonomiforvaltningen
3.1.3 Password opsætning (Kvantum) (gul)	Økonomiforvaltningen
3.2.1 Organisering af informationssikkerhed og styrkelse af ISMS (rød)	Økonomiforvaltningen
3.2.2 Gennemgang af rettigheder (Kvantum) (gul)	Økonomiforvaltningen
3.2.3 Sikkerhedsvurdering af systemer (rød)	Økonomiforvaltningen, Socialforvaltningen

Revisionsbemærkning nr. 3.1.1 Tildeling af autorisationer (Kvantum)	
Farvemarkering (prioritet)	Rød
Gives til	Økonomiforvaltningen

Observationer og risici:
Vi har ved revisionen konstateret at en bruger har tildelt sig selv rettigheder (roller) i maj 2025 direkte i Kvantum og udenom IGA-løsningen. Det er oplyst at brugeren sidder i brugerstyring og har rettigheden til at tildele roller direkte i Kvantum. Tildeling af rettigheder direkte i Kvantum er endvidere ikke omfattet af ledelsestilsynet.
Der er risiko for uautoriseret tildeling af rettigheder, hvilket kan resultere i funktionsadskilles risici, tilsigtet og utilsigtet fejl m.v.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller til at tildeling af rettigheder i Kvantum sker gennem IGA-løsningen.	Økonomiforvaltningen

Handleplan januar 2026	Opfølgningsplan
Økonomiforvaltningen Brugerstyring har fulgt op på sagen, og der foreligger dokumentation af hele forløbet, herunder hvorfor medarbejderen tildelte rollen til sig selv. Brugerstyring har gennemgået hændelsen og genbesøgt proceduren med afdelingen for at sikre sig, at den korrekte proces følges fremadrettet, herunder at medarbejdere ikke må tildele sig selv rettigheder. Direkte manuelle tildelinger i Kvantum til slutbrugere vil blive fjernet af IGA-robotten. Derfor er alle tildelinger underlagt ledelsestilsyn. Handleplanen anses som gennemført.	**Økonomiforvaltningen** Handleplanen er gennemført

Revisionsbemærkning nr. 3.1.2 Adgang til at administrere batchjobs (Kvantum)	
Farvemarkering (prioritet)	Rød
Gives til	Økonomiforvaltningen

Observationer og risici:
Vi har ved revisionen konstateret en række brugere (4 fra KS og 22 fra KMD_UDV) med adgang til at administrere batchjobs i Kvantum.
Der er efterfølgende modtaget dokumentation for at der er foretaget en rolleændring efter vores analyse, samt det er oplyst at rolleændringen har reduceret adgangen til at administrere batchjobs i Kvantum.
Brugere med adgang til at administrere batchjobs har mulighed for at oprette, ændre eller slette jobs, hvilket medfører risiko for tilsigtet og/eller utilsigtet fejl, som kan påvirke forretningskritiske data.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**

Vi henstiller til at adgangen begrænses og primært søges udført gennem PIM-løsningen.	Økonomiforvaltningen

Handleplan januar 2026	Opfølgningsplan
Økonomiforvaltningen Som nævnt oven for er der foretaget en rolleændring, der stopper for, at almindelige brugere kan administrere batchjobs. Kun firefightere- eller PIM-brugere, der bliver logget, kan nu administrere batchjobs. Ændringen er gennemført hhv. d. 28. oktober (for KMD-brugere) og d. 4. november (for KS-brugere) 2025. Bemærkningen er med ovenstående handling gennemført.	**Økonomiforvaltningen** Handleplanen er gennemført

Revisionsbemærkning nr. 3.1.3 Password opsætning (Kvantum)	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen

Observationer og risici:
Vi har ved revisionen konstateret at en gruppe brugere (ZAUM_XXXXX) ikke følger Københavns Kommunes passwordpolitik. Brugerne er tilknyttet en special sikkerhedspolitik i Kvantum (BAC_USER), som er underlagt følgende profilparametre i Kvantum:

- "login/password_expiration time": Password udløb er sat til 999 dage.
- "login/password history size": Minimum password history er sat til 3

Manglende skift af password gør det nemmere for uautoriserede personer at gætte eller bryde adgangskoderne ved hjælp af brute force-angreb eller andre metoder. Et brute force-angreb er en metode, hvor en hacker forsøger at få adgang til en konto ved systematisk at prøve alle mulige kombinationer af adgangskoder, indtil den rigtige kombination findes.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Det anbefales, at passwordopsætningen følger Københavns Kommunes passwordpolitik, som stiller krav om at password skal skiftes efter maksimum 365 dage, og at password ikke kan genbruges før efter 24 password skift. Vi vil anbefale at I styrker adgangskodeparametrene, da der er en risiko for, at brugere kan tilgå SAP GUI direkte og få adgang til ZAUM_XXXX brugerne. SAP GUI (Graphical User Interface) er den primære grænseflade, som brugere anvender til at interagere med SAP-systemet. Det er et program, der installeres på brugerens computer og giver adgang til SAP-applikationer og data. Hvis brugerne omgår Single Sign-On (SNC) og logger ind direkte på SAP GUI, kan de potentielt undgå de sikkerhedsforanstaltninger, der er forbundet med Single Sign-On via AD. Derfor er det vigtigt at sikre, at adgangskoderne i SAP GUI også er stærke og komplekse for at beskytte systemet mod uautoriseret adgang, herunder at generiske brugere med svage password i Kvantum misbruges.	Økonomiforvaltningen

Handleplan januar 2026	Opfølgningsplan
Økonomiforvaltningen SAP Kompetencecenter (SKC) har d. 25. november 2025 implementeret KMDs sikkerhedspolitik for passwords. Ændringsintervallet er på 365 dage, og passwords-længden er sat til 30 karakterer. SNC er ikke implementeret for Kvantum, og brugerne kan derfor ikke omgå denne, når de logger på SAP GUI.	**Økonomiforvaltningen** Handleplanen er gennemført

Bemærkningen er med ovenstående handling gennemført.	

Revisionsbemærkning nr. 3.2.1 Organisering af informationssikkerhed og styrkelse af ISMS	
Farvemarkering (prioritet)	Rød
Gives til	Økonomiforvaltningen

Observationer og risici:

Siden 2021 har revisionen løbende påpeget behovet for at styringen og gennemsigtigheden af arbejdet med informationssikkerhed i KK, skal styrkes væsentligt.

Dertil kommer, at nye lovgivninger og reguleringer (aktuelt NIS2, AI Act og forventede yderligere reguleringer de kommende år) kræver en større grad af gennemsigtighed, hvor ledelsen vil blive afkrævet svar om prioriteringer, dokumentation og det ledelsesmæssigt vedtagne sikkerhedsniveau hvilket bl.a., kræver at KK har et ISMS.

Opfølgning 2025

Der er udarbejdet en handleplan for første fase frem til marts 2026, der afsluttes med et 'stop and go' med beslutning om næste fase. Det er forventningen, at ISMS-implementeringen vil forløbe over 3 år, hvor delelementer løbende vil overgå til drift og øge den ledelsesmæssige gennemsigtighed omkring informationssikkerheden.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Det henstilles, at arbejdet gennemføres hurtigst muligt således, at den periode hvor den øverste ledelse må acceptere et, "uklart" billede af den samlede informationssikkerhed, herunder manglende viden om foranstaltninger og effektiviteten af kontroller samt residualrisikoen, reduceres mest muligt.	Økonomiforvaltningen

Handleplan januar 2026	**Opfølgningsplan**
Økonomiforvaltningen Bemærkningen er også givet i Revisionsberetning vedr. årsregnskab 2024, hvorfor handleplanen herfra gentages her, mens der gives status for arbejdet i opfølgningskolonnen. Handleplanen består af tre delelementer, som beskrives nedenfor: 1) ISMS, 2) Implementering af CIS18-kontroller, 3) It-anskaffelsesprocessen. <u>1. ISMS</u> Implementering af et ISMS i KK følger den handleplan, der blev godkendt af It-kredsen i Q2 2025. Handleplanen afsluttes med 'stop and go', hvor der tages stilling til næste fase i programmet (fase 2). Denne tilgang er valgt for at sikre, at erfaringer løbende tages op på rette ledelsesniveau mhp. evt. tilpasninger af programmet. Arbejdet ledes af CISO-funktionen i ØKF, som har nedsat en række arbejdsgrupper med repræsentanter fra forvaltningerne med ansvar for at omsætte de af ledelsen udpegede fokusområder til konkrete initiativer, der skal implementeres i forvaltningerne. Deadline for første fase: Q1-2026. Forventet deadline for den samlede implementering af et ISMS i KK: Q3 2028.	**Økonomiforvaltningen** <u>1. ISMS</u> Implementeringen følger tidsplanen for fase 1. Styregruppen har godkendt en række leverancer, herunder prioritering af NIS2 foranstaltninger, beskrivelse af de væsentligste roller (opgaver) i informationssikkerhedsarbejdet, awareness-tiltag mv. Parallelt arbejdes der på at etablere grundlaget for en systematisk tilgang til styringen af informationssikkerhedsrisici på tværs af KK. Projektgrundlag for fase 2 af programmet udarbejdes januar/februar 2026, opdelt i hvad der i løbet af fase 2 skal implementeres fra fase 1, og hvad der skal videreudvikles, herunder også ift. fasens varighed. Initiativer vedr. målepunkter og ledelsesrapportering vil blive anbefalet prioriteret, som et af udviklingssporene i fase 2. Yderligere vil der i takt med implementeringen af GRC-systemet kunne udarbejdes rapporter til ledelsen om complianceniveauet. Stop and go tilgangen til programmet fortsættes, hvorfor der ved udgangen af fase 2 tages stilling til det videre arbejde. <u>2. Implementering af CIS18-kontroller</u> A) Koncern IT har sammen med forvaltningerne afdækket, hvor og hvilken it-infrastruktur, der driftes

2. Implementering af CIS18-kontroller CIS18 er ligesom ISO27001 et rammeværk, der sikrer en standardiseret tilgang til sikkerhedsniveauet. CIS18 er målrettet it-infrastruktur og er et rammeværk, som ØKF har arbejdet med i vurderingen af den tværgående it-infrastruktur i KK, som forvaltningen varetager. Med revisionsbemærkningen sættes fokus på at sikre en standardiseret tilgang til al it-infrastruktur i KK. A) Afdækning af it-infrastruktur Det afdækkes hvor og hvilken it-infrastruktur, der driftes i KK. Deadline: Q4 2025. B) Udarbejdelse af fælles tilgang til CIS18-kontroller CIS18 rammeværket består af en række kontroller, hvor nogle er mere relevante end andre for KK som organisation. På baggrund af afdækningen af it-infrastrukturen i KK tages der stilling til KK's samlede tilgang til CIS18, herunder om behov for en differentieret brug af CIS18 grundet forskelligartet it-infrastruktur og formål hermed samt governance for arbejdet med CIS18. Deadline: Q1-2026. C) Forvaltningsspecifik implementering af CIS18-kontroller Når pkt. A og B er gennemført, vil KK have grundlaget for at vurdere, hvordan CIS18-kontroller kan implementeres i de omfattede forvaltninger mhp. forvaltningsspecifikke handle- og implementeringsplaner herfor. I den forbindelse tages også stilling til en endelig deadline for implementering af CIS18 i KK. ØKF har en igangværende implementeringsplan for risikovurdering af den tværgående KK it-infrastruktur varetaget af forvaltningen med udgangspunkt i CIS18. Dette arbejde fortsætter parallelt med ovenstående og forventes at vare 2027 ud. 3. It-anskaffelsesprocessen følger ISO-krav ØKF har igangsat et projekt, der skal genbesøge it-anskaffelsesmodellen i kommunen mhp. at skabe bedre forudsætninger for at arbejde differentieret og risikobaseret med it-anskaffelser. Inden udgangen af Q3-2025 vil det blive undersøgt, hvordan kravene fra ISO'erne, herunder 27001 Anneks A, kan blive indarbejdet i den nye model. Deadline: Q1 2026. Deadline for samlet handleplan: Q3-2028.	i KK. Der afrapporteres herpå til Teknisk Forum, Digitaliseringschefkredsen og It-kredsen i hhv. januar og februar. B) Det er fortsat planen at udarbejde KK's samlede tilgang til CIS18 i Q1 om end governance ikke forventes at være på plads i Q1. Vedr. den tværgående infrastruktur, som Koncern IT er ansvarlig for, er der implementeret en forvaltningsspecifik forretningsgang for risikovurdering og rapportering af it-infrastruktur vha. CIS18 kontrollerne. Erfaringerne fra dette arbejde vil indgå i punkt B og C. 3. It-anskaffelsesprocessen følger ISO-krav ØU har godkendt nyt forretningscirkulære for it-anskaffelser, som skal træde i kraft samtidig med ny forretningsgang, som forventes klar i 2026. Kravene fra relevante ISO'er indarbejdes i regi af arbejdet med hhv. kravrepositorium om den nye forretningsgang.

Revisionsbemærkning nr. 3.2.2 Gennemgang af rettigheder (Kvantum)	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen

Observationer og risici:

Tildelingen af rettighederne "Lederhat" og "Prokuraværdi" sker manuelt via brugeradministration i Kvantum. Disse rettigheder er ikke omfattet af den automatiske tildelingsproces, der håndteres af Omada. Dette betyder, at tildelingen af disse specifikke roller ikke følger den samme automatiske proces som andre roller, der administreres automatisk.

Vi har fået oplyst, at Omada indeholder oplysninger om de tildelte rettigheder, og at det periodiske ledelsestilsyn af de nævnte rettigheder basere sig på en rapport fra Omada og ikke fra Kvantum.

Det har i forbindelse med revisionen ikke været muligt for os at opnå overbevisning om at udtrækket fra Omada er fuldstændigt og nøjagtigt i forhold til de nævnte rettigheder. Det er derfor ikke muligt at vurdere om listen som anvendes til gennemgangen, er fuldstændighed og nøjagtighed.

Opfølgning 2025

Der er ved revisionen konstateret at "Lederhat" og "Prokuraværdi" fortsat ikke er inkluderet i ledelsestilsynet, dog er der foretaget en manuel kontrol forud for ledelsestilsynet, hvor brugere med "Lederhat" og "Prokuraværdi" er gennemgået. For den manuelle kontrol der er udført, foreligger ikke dokumentation for fuldstændighed og nøjagtighed af datagrundlaget der er anvendt til kontroludførslen. Vi er endvidere blevet informeret om at der arbejdes på at implementere løsning for tildelinger via IGA.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi anbefaler, at der som led i den periodiske gennemgang laves en afstemning af oplysningerne i Omada og Kvantum for de nævnte rettigheder, da der en forhøjet risiko for fejl i integrationen ved manuelle tildelinger direkte Kvantum.	Økonomiforvaltningen

Handleplan januar 2026	Opfølgningsplan
Økonomiforvaltningen SAP Kompetencecenter (SKC) er ved at undersøge mulighederne for en automatisering via Business Technology Platform (BTP). For nuværende ser det realistisk ud. På baggrund af undersøgelserne designes og implementeres processer, der er systemunderstøttet. Forventes afsluttet med udgangen af 2026.	**Økonomiforvaltningen** SKC inviterer Intern Revision til en gennemgang af den designede løsning i Q2 2026. Implementeringsplan forventes færdig i Q3 2026.

Revisionsbemærkning nr. 3.2.3 Sikkerhedsvurdering af systemer	
Farvemarkering (prioritet)	Rød
Gives til	Økonomiforvaltningen, Socialforvaltningen

Observationer og risici:
Sikkerhedsvurdering af systemer
Af Forretningscirkulæret for IT-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt IT-system skal sikkerhedsvurderes, inden det idriftsættes.

I 2023 konstaterede vi at der er, jf. oplysningerne i FISKK, er mange systemer, som er anskaffet før 1. november 2018, der ikke har en ibrugtagningsstatus, og at flere systemer har en "ikke godkendt" status.

Forvaltningernes har igangsat en handleplan som omfatter:
1. KIT foretager en tilpasset sikkerhedsvurdering af
    a. it-systemer i drift fra før 2018, *der har undergået væsentlige ændringer*,

b. it-systemer ibrugtaget før 2018 uden ibrugtagningstilladelse, men hvor der efterfølgende er foretaget en risikovurdering,

2. KIT gennemgår systemer registreret som "ikke godkendt" i FISKK og går i dialog med relevante forvaltninger om nødvendighed af eskalation, ny sikkerhedsvurdering eller udfasning af ikke-godkendte it-systemer.

Status 2025
ØKF oplyser, at handleplanen næsten er gennemført. Forvaltningerne mangler at klarmelde 2 systemer til sikkerhedsvurdering hos KIT.
I Q4 2025 vil ØKF eskalere systemer med status "Ikke godkendt".

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
I lighed med tidligere år henstilles det, at ► der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018, samt, ► de systemer, der har status "ikke godkendt" eskaleres, jf. anskaffelsescirkulæret, og der træffes de nødvendige foranstaltninger, bl.a. om udfasning, idet disse, jf. kommunes regler, udgør en sikkerhedsrisiko.	Økonomiforvaltningen, Socialforvaltningen

Handleplan januar 2026	**Opfølgningsplan**
Socialforvaltningen Socialforvaltningen har tre systemer under udfasning, som ikke har en ibrugtagningstilladelse. Forvaltningen vil hurtigst muligt sikre, at de tre systemer udfases og lukkes hurtigst muligt, senest med udgangen af 3. kvartal 2026. • Socialforvaltningen arbejder aktuelt på en dispensationssag for manglende ibrugtagningstilladelse og manglende onboarding i IGA, som IT-kredsen orienteres skriftligt om i 1. kvartal 2026. • FISKK#3150 (SOF Regnskab, Mellemkommunal refusion) har skiftet status i FISKK fra at være i status *Drift* til at være i status *Planlagt udfaset* i FISKK og udfases helt i start januar 2026 • FISKK#1629 (FITOutcomes) og FISKK#2124 (OpenFIT) har skiftet status i FISKK fra at være i status *Drift* til at være i status *Planlagt udfaset* i FISKK. Socialforvaltningen annoncerer i januar 2026 et udbud med henblik på anskaffelse af et nyt samlet system til den evidens baserede metode Feedback Informed Treatment (FIT) i 2. kvartal 2026 og dermed kunne udfase FISKK#1629 og FISKK#2124 i 3. kvartal 2026. I forvaltningens arbejde med at udarbejde handleplanen, er vi blevet opmærksom på yderligere et system uden ibrugtagningstilladelse, hvorfor der er 3 systemer der ikke opfylder kravene i Forretningscirkulæret for IT-anskaffelser. Det	**Socialforvaltningen** • IT-kredsen orienteres om dispensationssagen. Der vil ske opfølgning på dette med udgangen af 1. kvartal 2026, hvorvidt dette er foretaget. • FISKK#3150 udfases og lukkes. Der vil ske opfølgning med udgangen af januar 2026, hvorvidt dette er foretaget. • FISKK#1629 og FISKK#2124 udfases og lukkes. Der vil ske opfølgning 3. kvartal 2026, hvor vidt dette er sket, ligesom der vil ske opfølgning på det annoncerede udbud i januar 2026 om et nyt system er blevet valgt. Det vil ske med udgangen af 2. kvartal 2026.

tilkomne 3. system FISK 3150 bliver dog udfaset og lukket med udgangen af januar 2026. Handleplanen forventes færdiggjort med udgangen af 3. kvartal 2026.	
Økonomiforvaltningen Bemærkningen er også givet i Revisionsberetning vedr. årsregnskab 2024, hvorfor handleplanen herfra gentages her, mens der gives status for arbejdet i opfølgningskolonnen. Pkt. 1 Koncern IT vil forelægge Digitaliseringschefkredsen en sag med forslag til proces for opdatering af deres it-systemoplysninger i KK's it-systemregister (FISKK) for it-systemer uden ibrugtagningsstatus. Sagen vil indeholde en oversigt over it-systemer uden ibrugtagningsstatus samt en deadline for opdateringen. Pkt. 2 KK har implementeret en række tekniske foranstaltninger, herunder netværkssegmentering, udvidet pc-beskyttelse, anomaliovervågning mv., der nedsætter risikoen for kommunes ældre it-systemer (it-systemer fra før 2018). Koncern IT vil gennem Digitaliseringschefkredsen sætte fokus på kravet om sikkerhedsvurdering af it-systemer i drift fra før 2018, der har undergået væsentlige ændringer, og ud fra en risikobetragtning bede dem indmelde relevante it-systemer til en tilpasset sikkerhedsvurdering, hvor Koncern IT i samarbejde med de givne forvaltninger vurderer det konkrete behov ud fra it-systemets kritikalitet set ift. de implementerede tekniske foranstaltninger. Pkt. 3 I samarbejde med de it-systemansvarlige i forvaltningerne vil Koncern IT gennemføre den tilpassede sikkerhedsvurdering af de it-systemer, forvaltningerne indmelder som følge af punkt 2. For it-systemer ibrugtaget før 2018 uden ibrugtagningstilladelse, men hvor der efterfølgende er foretaget en risikovurdering, vil denne indgå i den tilpassede sikkerhedsvurdering Pkt. 4 Koncern IT gennemgår registreringer markeret med "ikke godkendt" i FISKK og går i dialog med relevante forvaltninger om nødvendighed af eskalation, ny sikkerhedsvurdering eller udfasning af ikke-godkendte it-systemer. **Deadline** Q3 2026	**Økonomiforvaltningen** Pkt. 1 Punktet er lukket. Pkt. 2-4 Med undtagelse af tre it-systemer i Socialforvaltningen, som senest forventes udfaset i løbet af Q3 2026, jf. forvaltningens handleplan herfor, er alle de it-systemer, der blev identificeret til at mangle ibrugtagningstilladelse som følge af bemærkningen, afklaret. Økonomiforvaltningen understøtter i Q1 2026 Socialforvaltningen i at søge dispensation for fortsat drift hos It-kredsen indtil it-systemerne kan udfases. Som led i at sikre, at KK-reglerne overholdes ift. at it-systemer ikke må sættes i drift uden ibrugtagningstilladelse, vil Koncern IT kvartalsvist med udgangspunkt i data fra kommunens it-systemregister udsende en opfølgning til forvaltningernes digitaliseringskontorer. Første oversigt udsendes Q1 2026.