

Bilag 5: Handleplaner til revisionsbemærkninger den løbende revision 2024

Dette bilag gennemgår handleplanerne for den løbende revision 2024. Bilaget følger den fællesskabelon, som udsendes af Økonomiforvaltningen (ØKF). Bilaget sendes til ØKF som led i deres konsolidering af opfølgningen på den løbende revision.

Den første tabel i bilaget er en oversigt over samtlige revisionsbemærkninger i forbindelse med den løbende revision. De revisionsbemærkninger, som er relevante for Kultur- og Fritidsforvaltningen, er farvet grønne. I forbindelse med den løbende revision for 2024 er 3 af 19 revisionsbemærkninger relevante for Kultur- og Fritidsforvaltningen.

De efterfølgende tre tabeller er gennemgang af de enkelte revisionsbemærkninger, som er relevante for Kultur- og Fritidsforvaltningen. Gennemgangen er indledes af tre afsnit, som er udarbejdet af Økonomiforvaltningen: Observationer og risici, revisionsmærkning samt handleplan. Handleplanen har ØKF taget fra forvaltningernes tidligere indmeldinger, som har været udvalgsgodkendt. Det skal bemærkes, at revisionsbemærkningerne vedrørende revision af løn- og personaleområdet er så nye, at de ikke tidligere har været udvalgsbehandlet, og derfor er handleplanerne udfyldt af forvaltningerne.

Det sidste afsnit – status januar 2025 – udarbejdes af forvaltningerne. Da der er tale om revisionsbemærkninger for den løbende revision for 2024, vil der være bemærkninger, som allerede er håndteret. For de revisionsbemærkninger, der ikke er håndteret, gives der status på processen samt tidsfrist for udførelse af handleplanen.

Bemærkninger i den løbende revision vedr. Regnskabsføring, forretningsgange og interne kontroller 2024	
3.1.1.1 Administration af autorisationer til Kvantum (rød)	Økonomiforvaltningen
3.1.1.2 Administration af autorisationer til Kvantum (gul)	Økonomiforvaltningen
3.1.2.1 Bilagskontrol (gul)	Børne- og Ungdomsforvaltningen, Socialforvaltningen
3.1.2.2 Bilagskontrol (grøn)	Sundheds- og Omsorgsforvaltningen, Teknik- og Miljøforvaltningen, Økonomiforvaltningen
3.2.1.1 Brugeradministration Kvantum (SAP Basis) (rød)	Økonomiforvaltningen
3.2.1.2 Brugeradministration (privilegerede brugere) (gul)	Økonomiforvaltningen
3.2.2.1 Kreditor (grøn)	Forvaltningerne
Bemærkninger i den løbende revision vedr. Generelle IT-kontroller 2024	
3.1.1 Organisering af informationsikkerhed og styrkelse af ISMS (rød)	Økonomiforvaltningen
3.1.2 Risikovurderinger af it-systemer (rød)	Økonomiforvaltningen
3.1.3 Åbning af det produktive miljø (Kvantum) (rød)	Økonomiforvaltningen
3.1.4 Log af åbninger (Kvantum) (rød)	Økonomiforvaltningen
3.1.5 Password opsætning (Kvantum) (gul)	Økonomiforvaltningen
3.1.6 Gennemgang af rettigheder (Kvantum) (gul)	Økonomiforvaltningen
3.2.1 Ledelsestilsyn med bruger autorisationer (rød)	Forvaltningerne
3.2.2 Sikkerhedsvurdering af systemer	Forvaltningerne
Bemærkninger i den løbende revision vedr. Revision af løn- og personaleområdet 2024	
4.4 Afregning til Feriefonden (rød)	Forvaltningerne
4.1 Arbejdsskade (gul)	Økonomiforvaltningen
4.3 Sagsgennemgang (grøn)	Økonomiforvaltningen
4.2 VIP-kontrol (grøn)	Økonomiforvaltningen

3.2.1 Ledelsestilsyn med bruger autorisationer	
Farvemærkning (prioritet)	Rød
Gives til	Forvaltningerne

Observationer og risici:

Ledelsestilsyn med brugerautorisationer

Det er i KK besluttet, at IT-systemer med adgangsstyring, som håndterer person- eller værdioplysninger, skal integreres med kommunens til enhver tid anvendte brugerstyringsløsning til bestilling af autorisationer.

Hvis integration til den gældende brugerstyringsløsning fravælges, skal fravalget dokumenteres og forelægges for ØKF, som efter koordinering med IT-kredsen kan meddele dispensation herfra. Det sker ikke konsekvent i dag.

Kommunen skal føre en ajourført fortegnelse over alle væsentlige informationsaktiver.

I KK er fortegnelsen i FISKK og indeholder ca. 1.400 informationsaktiver/systemer, som kan være infrastrukturelementer, systemer m.v.

Det skal aktivt sikres, at informationer er korrekt mærkede i forhold til det fastlagte dataklassifikationssystem med henblik på at leve op til gældende regler.

Forvaltningerne oplyser, at der er stor usikkerhed omkring de registrerede oplysninger i FISKK, som systemejerne har til opgave at ajourføre.

Systemer integreret i kommunens IGA-løsning inddeles efter kritikalitet, hvor der for systemer med person- og værdioplysninger skal udføres manuelt tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov, minimum hvert år eller hvert andet år. Forvaltningerne har oplyst, at ledelsestilsyn ikke fuldt ud er udført i overensstemmelse med reglerne, og at udeståender er planlagt gennemført hurtigst muligt.

For en stor del af systemerne med brugere eller som håndterer person- eller værdioplysninger, er den valgte brugerstyringsløsning fravalgt eller ikke teknisk mulig.

Det betyder som udgangspunkt, at der hver 6. måned manuelt skal foretages tilsyn med, om tildelte autorisationer afspejler medarbejdernes arbejdsmæssige behov. Ifølge forvaltningernes oplysninger foretages de halvårlige tilsyn med tildelte autorisationer kun i mindre grad.

Endelig ses der ikke at være taget stilling til, hvordan de væsentlige strategiske mål og forretningsmæssige gevinster, der sikres i IGA-løsningen, sikres for systemer uden for IGA-løsningen.

Status 2024

Forvaltningernes har besluttet og igangsat en handleplan som omfatter:

1. Udførelse af ledelsestilsyn, jf. KK's regler
2. Korrekt mærkning i forhold til det fastlagte dataklassifikationssystem i kommunens fortegnelse FISKK
3. Onboarding af systemer i brugerstyringsløsningen
4. Genbesøg af informationssikkerhedscirkulæret
5. Fortsættelse af igangværende udviklingsopgaver mhp. Effektiv administration.

Handleplanen forventes gennemført i perioden Q4 2024 til ultimo 2025.

Revisionsbemærkning:

Bemærkningen videreføres og i lighed med tidligere år henstilles til, at:

- de ledelsestilsyn, som skal sikre, at de ansatte ikke har adgang til personoplysninger, hvor der ikke er et arbejdsbetinget behov, udføres i overensstemmelse med kommunens regler. Det gælder både de systemer, der er integreret i IGA-løsningen, og de systemer, der ligger uden for IGA-løsningen
- det aktivt sikres, at systemer er korrekt mærkede i forhold til det fastlagte dataklassifikationssystem i kommunens fortegnelse FISKK
- alle kommunens systemer med adgangsstyring og værdi- og personoplysninger, hvis det er teknisk muligt, integreres i kommunens IGA-løsning
- der tages stilling til, hvordan de væsentlige strategiske mål og forretningsmæssige gevinster, der sikres i IGA-løsningen, sikres for de 587 systemer, som på nuværende tidspunkt ikke er i IGA-

Berørt(e) forvaltning(er):

Forvaltningerne

løsningen, og de 39 systemer, hvor det ikke teknisk er muligt at blive tilmeldt IGA-løsningen, bør være særligt kritiske.

Det anbefales herudover, at:

- ledelsestilsynene for systemer integreret i kommunens IGA-løsning opstartes automatisk
- Kommunens regler (governance) revurderes og beskrives i en fælles administrativ forretningsgang, hvor der fokuseres på at skabe gennemsigtighed i hvordan og hvilke strategiske mål og forretningsmæssige gevinster, der operationaliseres/sikres for fuldt ud at realisere målet om at reducere ressourceforbruget på området væsentligt og forbedre brugeroplevelsen for autorisationsansvarlige og ledere.

Handleplan	Status januar 2025
<p>Kultur- og Fritidsforvaltningen Intern revision henstiller at:</p> <p>1. Ledelsestilsyn skal udføres i overensstemmelse med kommunens regler:</p> <p>KFF gennemfører i overensstemmelse med kommunens regler ledelsestilsyn med autorisationer årligt for systemer i Identity Governance & Administration (IGA), senest november 2023 og halvårligt for systemer udenfor IGA, senest marts 2024.</p> <p>2. Systemer skal være korrekt mærkede ift. det fastlagte dataklassifikations-system i kommunens fortegnelse FISKK:</p> <p>KFF sikrer sig løbende at forvaltningens systemer er korrekt opmærkede i arbejdet med årsplanerne i FISKK. Senest har systemejerggruppen i april måned 2024 systematisk gennemgået deres systemer ift. registrering af datatyper i systemet.</p> <p>3. Alle kommunens systemer med adgangsstyring og værdi- og personoplysninger, skal, hvis det er teknisk muligt, integreres i kommunens IGA-løsning:</p> <p>KFF igangsætter en handleplan, der skal sikre, at forvaltningens systemer med adgangsstyring og værdi- og personoplysninger, hvis det er teknisk muligt, integreres i kommunens IGA-løsning.</p> <p>Handleplanen afdækker tekniske forudsætninger for systemerne og konkret økonomi for det enkelte system samt sikrer, at der udarbejdes en konkret plan for at få lagt det pågældende system i IGA, hvis det er teknisk muligt.</p> <p>4. Der skal tages stilling til hvordan de væsentlige strategiske mål og forretningsmæssige gevinster der sikres i IGA-løsningen, sikres for de systemer som på nuværende tidspunkt ikke er i IGA-løsningen.</p> <p>Dette forholder KFF sig også til i forbindelse med handleplanen nævnt ovenfor.</p>	<p>Kultur- og Fritidsforvaltningen</p> <p>Opfølgning:</p> <ul style="list-style-type: none">• Ad 1 Forvaltningen har imødekommet handleplanen. • Ad 2 Forvaltningen har imødekommet handleplanen. • Ad 3 KFFs handleplan, der skal sikre, at forvaltningens systemer med adgangsstyring og værdi- og personoplysninger, hvis det er teknisk muligt, integreres i kommunens IGA-løsning, fortsætter ind i 2025. • Ad 4 Dette forholder KFF sig til i forbindelse med handleplanen nævnt ovenfor. <p>Deadline for handleplan: Handleplanen skal være gennemført inden udgangen af 2025.</p>

<p>Intern revision anbefaler der ud over at:</p> <p>Ledelsestilsynene for systemer integreret i kommunens IGA-løsning bør opstartes automatisk samt at kommunens regler (governance) bør revurderes og beskrives i en Fælles administrativ forretningsgang med fokus på at skabe gennemsigtighed i, hvordan og hvilke strategiske mål og forretningsmæssige gevinster, der operationaliseres/sikres.</p> <p>KFF har en forventning om, at disse anbefalinger adresseres forvaltningstværgående og vil arbejde med dem i det regi.</p> <p><u>Deadline for handleplan:</u> 2025</p>	
---	--

3.2.2 Sikkerhedsvurdering af systemer	
Farvemarkering (prioritet)	Rød
Gives til	Forvaltningerne
<p>Observationer og risici:</p> <p><i>Sikkerhedsvurdering af systemer</i></p> <p>Af Forretningscirkulæret for IT-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt IT-system skal sikkerhedsvurderes, inden det idriftsættes.</p> <p>En sikkerhedsvurdering tager stilling til, at alle krav til informationssikkerhed og databeskyttelse er opfyldt. På baggrund af sikkerhedsvurderingen udstedes en ibrugtagningstilladelse. IT-systemer skal have en ibrugtagningstilladelse, inden de idriftsættes.</p> <p>Det er forbundet med stor risiko for kommunen at idriftsætte et IT-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse.</p> <p>I 2023 konstaterede vi, at der, 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. Altså skulle systemerne ikke være i drift, fordi sikkerheden ikke har levet op til kommunens krav.</p> <p>Status 2024</p> <p>Forvaltningernes har besluttet og igangsat en handleplan, som omfatter:</p> <ol style="list-style-type: none"> 1. KIT foretager en tilpasset sikkerhedsvurdering af <ol style="list-style-type: none"> 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 nødvendigheden af eskalation, ny sikkerhedsvurdering eller udfasning af ikke-godkendte IT-systemer. <p>Handleplanen forventes gennemført i perioden Q4 2024 til Q2 2025.</p>	
Revisionsbemærkning:	Berørt(e) forvaltning(er):
<p>Bemærkningen videreføres og i lighed med tidligere år henstilles det, at</p> <ul style="list-style-type: none"> ➤ de systemer, der ikke har en ibrugtagningsstatus, bliver gennemgået og oplysningerne i FISKK bliver opdateret. ➤ der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018. ➤ de systemer, der har status "ikke-godkendt" eskaleres, jf. anskaffelsescirkulæret, og der træffes de nødvendige foranstaltninger, 	Forvaltningerne

blandt andet om udfasning, idet disse, jf. kommunes regler, udgør en sikkerhedsrisiko.	
Handleplan	Status januar 2025
<p>Kultur- og Fritidsforvaltningen Revisionsbemærkningen gælder alle forvaltninger.</p> <p>I forlængelse af revisionsbemærkningen om overholdelse af reglerne for ibrugtagning af it-systemer, som ØKF fik ifm. de generelle it-kontroller 2023 og den handleplan, ØKF udarbejdede i forlængelse af denne, har KFF gennemgået og opdateret felter i FISKK for 37 systemer.</p> <p>KFF afventer tilbagemelding fra ØKF, hvor systemerne opdeles efter ny kritikalitetsscore, hvorefter KFF kan få udført tilpasset sikkerhedsvurdering af Koncern It.</p> <p>KFF har ingen systemer med status "ikke godkendt" i FISKK.</p> <p>KFF har på baggrund af den øgede opmærksomhed på korrekt registrering lavet en undersøgelse af dette i efteråret 2023. Her fandt Digitaliseringskontoret en række it-systemer, der ikke er registreret i FISKK. Digitaliseringskontoret er ved at undersøge, hvilke der skal registreres og hvilke der kan afskaffes. Systemer, der skal registreres, bliver registreret i FISKK og der igangsættes sikkerhedsgodkendelse. En gennemgang har vist, at der er tale om mindre støttesystemer, der hverken behandler borgerdata eller værdidata. Det er f.eks. systemer til lys- og lydstyring i kulturinstitutioner. Efter årsskiftet etableres tekniske systemejerskaber for de relevante systemer.</p> <p><u>Deadline for handleplan:</u> Det er som en del af ØKFs handleplan til revisionen meddelt, at arbejdet kan være gennemført mellem Q4 2024 og Q2 2025. KFF følger denne handleplan.</p>	<p>Kultur- og Fritidsforvaltningen</p> <p>Opfølgning:</p> <ul style="list-style-type: none"> • KFF følger stadig op i regi af ØKFs handleplan, hvilket i praksis betyder, at KFF får sikkerhedsvurderet de systemer, der fremgår af ØKFs tilbagemelding. KFF har pt. 7 systemer til sikkerhedsvurdering. • It-anskaffelsesprocessen, inkl. risikovurdering, er under revision med KIT for bordenden, og KFF følger dette arbejde og efterlever processer og værktøjer, efterhånden som de bliver færdige. • I relation til de fundne systemer udenfor FISKK har KFF nu skaffet sig af med de systemer, der ikke længere skal benyttes og får lagt de systemer, der fortsat skal benyttes, i FISKK i starten af det nye år. <p>Deadline for handleplan: Q2 2025</p>

4.4 Afregning til Feriefonden	
Farvemarkering (prioritet)	Rød
Gives til	Forvaltningerne
<p>Observationer og risici: Vi har konstateret, at der er fejl i grundlaget for de 6 mio. kr. som KK har afregnet til Feriefonden i 2023 for optjeningsåret 2021/2022.</p> <p>Helt overordnet er det vores opfattelse, at medarbejderne enten skal afholde deres ferie eller ferien skal overføres grundet feriehindring m.v. Således bør afregningen på medarbejderniveau typisk være på et uvæsentligt niveau.</p> <p>Vi har i samarbejde med KS foretaget en gennemgang af de 10 højeste afregninger. Gennemgangen viser fejlagtige afregninger, der kan henføres til KS og overvejende sandsynlig, fejlagtig administration i forvaltningerne.</p> <p>Væsentlige afregninger på medarbejderniveau kan typisk henføres til ikke-indberettet ferie, hvilket medfører en dobbeltudgift for KK eller fejl i håndteringen af ferie i forbindelse med fratrædelser, feriehindring m.v., som medfører mistet ferie for medarbejderne.</p>	

<p>Der er medio november 2024 afregnet 4,5 mio. kr. til Feriefonden vedr. optjeningsåret 2022/2023. På baggrund af vores observationer, jf. ovenfor, har KS nået at berigtige 0,5 mio. kr. De konstaterede fejl understøtter vores vurdering af, at der er væsentlige fejl i håndteringen af medarbejdernes ferie, der medfører fejlagtig afregning til Feriefonden.</p>	
<p>Revisionsbemærkning:</p> <p>KS har tilrettelagt og implementeret flere fornuftige tiltag, der skal medvirke til at sikre en korrekt håndtering af ferie i forvaltningerne.</p> <p>Det er vores vurdering, at de tilrettelagte processer ikke er tilstrækkeligt effektive i forhold til at sikre mod fejl i håndteringen af medarbejdernes ferie. For at sikre, at medarbejderne får overført den ferie de er berettiget til, og at KK ikke får et økonomisk tab, henstiller vi til, at KS i samarbejde med forvaltningerne tilrettelægger en mere effektiv proces.</p> <p>Desuden henstiller vi til, at KS så vidt muligt berigtiger de konstaterede fejl, der kan henføres til KS.</p>	<p>Berørt(e) forvaltning(er):</p> <p>Forvaltningerne</p>
<p>Handleplan januar 2025</p> <p>Kultur- og Fritidsforvaltningen</p> <p>Kultur- og Fritidsforvaltningen håndterer risikoen for fejl i ferie ved hjælp af en forvaltningsspecifik vejledning for kontrol af ferie, som findes på Kultur- og Fritidsforvaltningen intranet og som sendes ud via Kultur- og Fritidsforvaltningen lederpakke forud en kontrol med ferie. Den lokale leder har ansvar for at sikre, at kontrollen, som er beskrevet i den forvaltningsspecifikke vejledning, følges. Der skal foretages kontrol af ferie 3 gange om året, som beskrevet i vejledningen. Vejledningen er senest opdateret i 2024.</p> <p>Forvaltningen vil sammen med Koncernservice og de øvrige forvaltninger i regi af HR-kredsen afholde en workshop ultimo januar 2025 om håndtering af medarbejdernes ferie. Når koncernservice har udarbejdet løsningsforslag med henblik på implementering i Kultur- og Fritidsforvaltningen og de øvrige forvaltninger, vil Kultur- og Fritidsforvaltningen implementere relevante løsningsforslag.</p> <p>Deadline: Forvaltningen vil følge Koncernservice' tidsplan for implementeringen, forventelig deadline ultimo 2025.</p>	<p>Opfølgingsplan</p> <p>Kultur- og Fritidsforvaltningen</p> <p>Opfølgning:</p> <ul style="list-style-type: none"> Jf. handleplanen foretages der kontrol tre gange i 2025. Kultur- og Fritidsforvaltningen vil i 2026 følge op på, om de nye løsninger, der bliver implementeret i løbet af 2025, i tilstrækkelig grad sikre mod fejl i håndteringen af medarbejdernes ferie.