

Handleplaner til revisionsbemærkninger den løbende revision 2024

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 informationssikkerhed 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	
Farvemarkering (prioritet)	Rød
Gives til	Forvaltningerne
Observationer og risici:	
<p><i>Ledelsestilsyn med brugerautorisationer</i></p> <p>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.</p> <p>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.</p> <p>Kommunen skal føre en ajourført fortegnelse over alle væsentlige informationsaktiver.</p> <p>I KK er fortegnelsen i FISKK og indeholder ca. 1.400 informationsaktiver/systemer, som kan være infrastrukturelementer, systemer m.v.</p> <p>Det skal aktivt sikres, at informationer er korrekt mærkede i forhold til det fastlagte dataklassifikationssystem med henblik på at leve op til gældende regler.</p> <p>Forvaltningerne oplyser, at der er stor usikkerhed omkring de registrerede oplysninger i FISKK, som systemejerne har til opgave at ajourføre.</p> <p>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.</p>	

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 halvårige 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:	Berørt(e) forvaltning(er):
<p>Bemærkningen videreføres og i lighed med tidligere år henstilles til, at:</p> <ul style="list-style-type: none"> ➤ 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-løsningen, og de 39 systemer, hvor det ikke teknisk er muligt at blive tilmeldt IGA-løsningen, bør være særligt kritiske. <p>Det anbefales herudover, at:</p> <ul style="list-style-type: none"> ➤ 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. 	<p>Forvaltningerne</p>
Handleplan	Status januar 2025
<p>Beskæftigelses- og Integrationsforvaltningen BIF udfører ledelsestilsyn på sine systemer. Vi arbejder derfor på at forretningsmæssige systemer genbesøger de registrerede frekvenser og sikre, at de ajourført med gældende retningslinjer.</p>	<p>Beskæftigelses- og Integrationsforvaltningen</p> <ol style="list-style-type: none"> 1. I 2024 har forvaltningen igangsat og udført ledelsestilsyn som påkrævet i henhold til cirkulæret. I Q1 2025 overgår systemerne til automatisk igangsættelse af ledelsestilsyn. De

<p>Er systemer tilknyttet brugerstyringen udføres tilsyn hvert år. Er systemet ikke tilknyttet brugerstyringen, skal det foretages hvert 6 måned.</p> <p>Vi har indberettet en fælles oversigt til IGA-teamet pr. 19. juni for, hvornår vi planlægger at foretage ledelsestilsyn pr. system.</p> <p>Vi kommer til at følge op både i forhold til genbesøget af frekvens og udførelse af ledelsestilsynet.</p> <p>Systemer uden for IGA. BIF har 7 systemer uden for IGA. For de systemer, der ikke er under udfasning, vil forvaltningen genbesøge hvert enkelt system og påbegynde en onboardingproces med IGA, hvor det er muligt. For det ene system med uddelegeringsaftale skal det genbesøges, hvorvidt begrundelsen stadig holder.</p> <p>BIF har mange fællesoffentlige systemer, som er tilknyttet AD-brugerstyringen, men styres af FKA/FKO. Det er derfor ikke muligt at onboarder det til IGA. BIF tager derfor igen dialog med KIT, om de tekniske muligheder har ændret sig.</p> <p>BIF stiller krav ved anskaffelse af nye systemer, at de teknisk kan tilsluttes den centrale brugerstyringen og helst IGA. Når vi ikke kan stille krav om, at alle systemer skal kunne tilsluttes IGA, skyldes det, at BIF opererer med en del fællesoffentlige systemer, hvor KOMBIT/Staten har defineret brugerstyringsmulighederne. Da det er et lovkrav at være tilsluttet systemerne, kan vi ikke altid selv vælge, hvordan brugerstyring skal ske.</p> <p><u>Deadline for handleplan: Q3</u></p>	<p>4 systemer som har uddelegeringsaftaler, foresætter hvert 6. måned.</p> <p>2. Forvaltningen har løbende rettet mærkning og dataklassifikation på systemer i FISKK. Arbejdet vurderes som afsluttet.</p> <p>3. Onboarding af systemer i brugerstyring. Forvaltningen har udfaset tre systemer uden for IGA, samt genbesøgt et system med uddelegeringsaftale. Vi mangler at genbesøge et system, som forventes genbesøgt i januar grundet systemejerskiift.</p> <p>4. Forvaltningen har bidraget og afventer KIT endelige udkast og ØU's godkendelse.</p> <p>5. Forvaltningen bidrager aktivt til de KIT drevne projekter – herunder automatisk igangsættelse af ledelsestilsyn og udviklingen medarbejderroller.</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. 	
Handleplanen forventes gennemført i perioden Q4 2024 til Q2 2025.	
Revisionsbemærkning:	Berørt(e) forvaltning(er):
Bemærkningen videreføres og i lighed med tidligere år henstilles det, at <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. anskaffelses-cirkulæret, og der træffes de nødvendige foranstaltninger, blandt andet om udfasning, idet disse, jf. kommunes regler, udgør en sikkerhedsrisiko. 	Forvaltningerne
Handleplan	Status januar 2025
Beskæftigelses- og Integrationsforvaltningen Ibrugtagningsstatus og tilpasset sikkerhedsvurdering: BIF har tre systemer omfattet af revisionsbemærkningen. Vi skal i den forbindelse <ul style="list-style-type: none"> • Kritikalitetsscore systemerne • Fremskaffe og dokumentere systemerne. • Indmelde til sikkerhedsvurdering, når sikkerhedsvurderingen kan påbegyndes. <u>Deadline for handleplan: 31. juli 2024</u> Ikke godkendte systemer: BIF har 3 "ikke godkendte" systemer identificeret i revisionsbemærkningen. Vi skal i den forbindelse: <ul style="list-style-type: none"> • Udarbejde en udfasningsplan • Opsige kontrakter og lukke adgange • Sikre sletning. • Iværksætte udfasningen. <u>Deadline for handleplan: Q4 2024</u>	Beskæftigelses- og Integrationsforvaltningen <ol style="list-style-type: none"> 1. Ibrugtagningsstatus og tilpasset sikkerhedsvurdering, har forvaltningen indmeldt alle systemer til slutningen af januar 2025. Herefter er BIF færdige med indmeldingen. 2. BIF har udfaset 2 systemer, imens de sidste er under dispensationsbehandling på IT-K 31.1.2025. Herefter er forvaltningen færdig med handleplanen.

4.4 Afregning til Feriefonden	
Farvemærkning (prioritet)	Rød
Gives til	Forvaltningerne
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. 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. 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>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>	
Revisionsbemærkning:	Berørt(e) forvaltning(er):
<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>	Forvaltningerne
Handleplan januar 2025	Opfølgingsplan
Beskæftigelses- og Integrationsforvaltningen	Beskæftigelses- og Integrationsforvaltningen
<p>BIF vil i 2025 følge den udarbejdede opfølgingsplan fra Koncernservice med fokus på:</p> <ol style="list-style-type: none"> 1. særlig opmærksomhed på overførsel af ferie, når der er tale om feriehindring 2. at medarbejdere, der fratræder, får alt tilgodehavende ferie udbetalt 3. at de ledere, der har over kr. 10.000 i restferie, tager imod tilbuddet om at sparre med KS ift. fremtidig håndtering ift. restferie 4. rettidig godkendelse af indberettet ferie <p>HR i BIF har i 24, som et pilotforsøg, kontaktet medarbejdere med restferie direkte, og bedt dem planlægge resterende ferie.</p> <p>BIF vil, efter drøftelsen i HR -kredsen, tage stilling til, om tiltaget skal gentages og evt. justeres/udvides i 2025.</p>	<p>BIF vil i høj grad basere opfølgningen på handleplanen på tilbagemeldinger fra Økonomiforvaltningen ift. deres opfølgning.</p>