Handleplaner til Generelle IT-kontroller 2023

Bemærkninger i den løbende revision vedr. Revision af generelle IT-kontroller 2023	
3.1.1 Ledelsestilsyn med bruger autorisationer (rød)	Forvaltningerne
3.2.1 Ibrugtagning af it-systemer (rød)	Økonomiforvaltningen
3.2.2 Organisering af informationssikkerhed og styrkelse af det ISMS (gul)	Økonomiforvaltningen
3.2.3 Risikovurderinger (gul)	Økonomiforvaltningen

3.1.1 Ledelsestilsyn med bruger autorisationer	
Farvemarkering (prioritet)	Rød
Gives til	Forvaltningerne

Observationer og risici:
Ledelsestilsyn med bruger autorisationer
Det fremgår af cirkulæret for informationssikkerhed, at alle systemer, der ikke er integreret i IGA (Identity Governance & Administration), skal udføre ledelsestilsyn minimum hver 6 måned.

For systemer integreret i kommunens IGA-løsning inddeles systemer efter kritikalitet, hvor der henholdsvis skal udføres tilsyn, minimum hvert år eller hvert andet.

Af kommunens systemregister fremgår det, at der er et stort antal systemer, der behandler personoplysninger. Af disse er 245 systemer integreret i IGA.

Der er udtaget 25 stikprøver på systemer i IGA, hvor der er fastsat en frist for ledelsestilsyn og 25 for de systemer, hvor der ikke er fastsat frist. Alle de udvalgte systemer behandler følsomme personoplysninger jf. FISKK.

I flere tilfælde var der jf. oplysningerne i IGA-løsningen ikke udført eller påbegyndt et ledelsestilsyn.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Det henstilles, 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 med stor sandsynlighed også de systemer, der ligger uden for IGA-løsningen. Det anbefales, at ledelsestilsynene for systemer integreret i kommunens IGA-løsning opstartes automatisk. Det henstilles desuden, at alle kommunens systemer indeholdende værdi og personoplysninger, hvis det er teknisk muligt, integreres i kommunens IGA-løsning.	Forvaltningerne

Handleplan januar 2024	Opfølgning
Tværgående handleplan Der er over de seneste 8 år foretaget en løbende øget sikkerhed og effektivisering af administrationen af KK brugerautorisationer. Køb af en IGA løsning tilbage i 2016 har medført, at ca. 250 it-systemer er migreret og dermed ikke skal gennemføre manuelle tilsyn. Gevinsten heraf har været både i KIT og i de enkelte forvaltninger. På baggrund af erfaringer fra de seneste år har Koncern IT igangsat en række yderligere tværgående KK indsatser mhp. optimering af IGA-platformen og processer vedr. brugeradministration og ledelsestilsyn, som koordineres med forvaltningerne gennem Digitaliseringschefkredsen og It-kredsen. Disse tiltag er: Pkt. 1 Udarbejdelse af vejledning, der skal understøtte forvaltningerne i at forbedre rettighedsnavne, beskrivelser og	**Tværgående** *Ad 1-4* Digitaliseringschefkredsen og It-kredsen forelægges målbillede, katalog, tidsplan og organisering for arbejdet i Q1 2024 og bedes indmelde repræsentanter til en styregruppe, der skal sikre gennemførelse af tiltagene. *Ad 1* KIT udarbejder vejledning Q2 2024 hvorefter forvaltningernes gennem relevante kredse bedes igangsætte arbejdet med at forbedre autorisationsnavne og -beskrivelser samt tilføjer klassifikationer. *Ad 2* Format og proces for årshjul for automatisk igangsættelse af ledelsestilsyn forelægges styregruppen til godkendelse i Q4 2024, hvorefter automatisk igangsættelse af tilsyn vil køre for

klassifikationsmarkering af roller i brugerstyringsløsningen samt udarbejdelse af mere præcis og ensartet definition af autorisationer og adgangsniveauer mhp. at standardisere praksis og højne kvalitet. Pkt. 2 Opbygning af et årshjul for automatisk igangsættelse af ledelsestilsyn gennem IGA fremfor at systemejerne skal igangsætte tilsyn manuelt, hvorved det ikke vil afhænge af den enkelte systemejer, om der bliver ført tilsyn. Pkt. 3 Genbesøg af cirkulæretekst i forhold til hvilke it-systemer, der er behov for ledelsestilsyn af og hvor ofte der skal føres ledelsestilsyn baseret på kritikalitet og datatyper. Pkt. 4 I tillæg til ovenstående vil Koncern IT fortsat understøtte forvaltningerne i at migrere yderligere it-systemer til IGA-løsningen i 2024. Dette vil ske med udgangspunkt i genbesøg af cirkulæreteksten, jf. punkt 3, og forvaltningernes ønsker til onboarding af systemer. Koncern IT vil desuden genopfriske onboardning-processen overfor forvaltningerne gennem forskellig kommunikation. Som led i at forenkle det administrative arbejde, der følger af at gennemføre tilsyn, vil der sideløbende med ovenstående løbende blive implementeret og udbredt medarbejderroller, som kan tildeles medarbejdere automatisk, hvorved autorisationsansvarlige og ledere har færre autorisationer at forholde sig til ved ledelsestilsyn. **Deadline** Q4 2024	relevante it-systemer fra 2025 og frem og løbende blive udvidet og justeret. *Ad 3* Der er i regi af den nye KK Digitaliseringsstrategi igangsat et arbejde vedr. justering af it-styringsrammen bl.a. mhp. at understøtte en differentieret og risikobaseret tilgang til systemforvaltning, herunder krav om ledelsestilsyn. For så vidt angår ledelsestilsyn vil Forretningscirkulære for informationssikkerhed blive genbesøgt, når den overordnede linje for it-styring i kommunen er fastlagt mhp. godkendt justering senest Q4 2024. *Pkt. 4* Aktiviteterne forventes gennemført løbende henover 2024.
Beskæftigelses- og Integrationsforvaltningen Intern revision har identificeret to problemstillinger, som er relevant for kritikken i BIF. • Manglende dokumentation for gennemført tilsyn • Frister for tilsyn ikke overholdt. Forvaltningen vurderer, at begge kritikpunkter bunder i manglende konsekvent dokumentation for ledelsestilsyn. Vores handleplan har derfor fokus på at sikre dokumentation – og en systematisk indarbejdelse af tilsyn i årshjulet. **Handleplan** I forbindelse med omorganiseringen af BIF i foråret 2024 skal der foretages et ledelsestilsyn for alle systemer i BIF. • Der indføres derfor et fælles årligt ledelsestilsyn primo Q2 for alle systemer, samt i primo Q4 for systemer med halvårligt ledelsestilsyn. • KFD – team sikkerhed – udarbejder et samlet skema for hele BIF, hvor både bestilling, gennemførelse og resultat opdateres (marts). • Fristen for bestilling af tilsyn sættes til 1.april for alle systemejere. • Der følges op 15. april på, om ledelsestilsyn er igangsat. Hvis ikke, kontaktes IGA for at afklare udfordringer.	**Beskæftigelses- og Integrationsforvaltningen** Opfølgning i maj 2024 med en status til kontorchef i KFD. En endelig rapport til direktionen i ultimo maj med fokus på resultatet og evaluering af handleplan.

• Ved udgang af Q2 følges op på resultaterne. Her sikres dokumentationen, som gemmes i kopi samlet. • Skemaet skal bidrage til at identificere årsagerne til en eventuel forsinkelse kommer frem og kan håndteres. • BIF har to systemer udenfor IGA. Det ene er under udfasning. Det andet genbesøger vi de tekniske forudsætninger for at omstille systemet (FISKK # 3922) til en IGA-løsning. Deadline: 30. april 2024.	
Børne- og Ungdomsforvaltningen Forvaltningen har i 2023 igangsat følgende initiativer, der imødegår revisionens henstillinger og anbefalinger: • BUF har udarbejdet et årshjul, der dækker igangsættelse af ledelsestilsyn for både de tværgående it-systemer og væsentlige BUF-specifikke it-systemer. Ifølge årshjulet vil BUF i uge 9 og 37 igangsætte ledelsestilsynet. Ledelsestilsynet omfatter såvel systemer integreret i IGA-platformen som systemer udenfor. • BUF vil, med sparring fra KIT, lægge en plan for påbegyndelse af migrering af it-systemer, der endnu ikke er på IGA-platformen.	**Børne- og Ungdomsforvaltningen** Digitaliseringskontoret i BUF følger op på gennemførslen af ledelsestilsynet. Forvaltningens administrative fællesskaber understøtter og følger den enkelte leders gennemførsel af ledelsestilsynene decentralt. Der er godkendt en proces for eskalering af manglende gennemførsel af tilsyn til nærmeste leder.
Kultur- og Fritidsforvaltningen KFF har allerede forvaltningsspecifikke arbejdsgange for gennemførsel af ledelsestilsyn med autorisationer. En i relation til systemer hvor tilsynet foregår via IGA og en i relation til systemer, hvor tilsynet foregår udenfor IGA. Forvaltningen vil fortsat følge disse arbejdsgange. Ift. de to specifikke systemer, der er relateret til KFF; Terminal #4285 og Køreprøvebooking #383, har KFF følgende bemærkninger. • Terminal #4285 er begyndt implementeret i sommeren 2023 og er integreret i kommunens IGA-løsning. Ledelsestilsynet skal derfor gennemføres hver 12. måned og den frist er ikke overskredet endnu. Bemærkningen vedr. Terminal, er derfor ikke korrekt, hvilket Intern Revision vil blive gjort opmærksom på. • Køreprøvebooking #383. Der er gennemført manuelt tilsyn med systemet i marts 2023. Ledelsestilsynet skal gennemføres hver 6. måned. Fristen er derfor ikke overholdt. Der vil blive ført ledelsestilsyn med autorisationerne i systemet næste gang, der gennemføres tilsyn med systemer udenfor IGA, hvilket sættes i gang i marts 2024. KFF arbejder på at få lagt alle nye systemer ind i IGA og kigger samtidig på, ud fra en risikobaseret tilgang, hvilke af forvaltningens systemer udenfor IGA, der skal lægges over i IGA. **Deadline:**	**Kultur- og Fritidsforvaltningen** Forvaltningen følger fortsat sine forvaltningsspecifikke arbejdsgange for gennemførsel af ledelsestilsyn med autorisationer. **Opfølgning:** KFF vil igangsætte manuelt tilsyn med køreprøvebooking til marts 2024.

Der er deadline for gennemførelse af ledelsestilsyn på Køreprøvebooking #383 i marts måned 2024.	
Socialforvaltningen SOFs handleplan retter sig dels mod de tiltag, der er på vej fra KIT, og dels mod egne tiltag i SOF. KITs indsatser er følgende: • Forbedrede rettighedsnavne, beskrivelser og klassifikationsmarkering af roller med henblik på større klarhed over, hvad der reelt godkendes ved ledelsestilsynet. Selve autorisationer bliver også mere ensartet beskrevet og KIT vil kigge på cirkulæreteksten med henblik på, at få udvalgt de systemer til ledelsestilsyn, der er mest kritiske datatyper og forretningskritikalitet – tidshorisonten er ikke kendt • Implementering af automatisk tildelte medarbejderroller. Det giver færre autorisationer at forholde sig til, når der skal autoriseres og laves ledelsestilsyn – tidshorisonten er ikke kendt. • Opbygning af et fast årshjul for automatisk igangsættelse af ledelsestilsyn på autorisationer – tidshorisonten er ikke kendt Socialforvaltningen vil, i samarbejde med KIT, sikre implementering af KITs indsatser i forvaltningens drift. SOFs egne tiltag er følgende: • SOF er allerede i dialog med KIT med henblik på at få et overblik over systemer, der ikke er i IGA platformen og få lagt en plan for migrering af systemerne. Deadline er udgangen af 2. kvartal 2024, dog med forbehold for KITs ressourcer. • SOF arbejder med ledelsestilsyn ud fra en risikobaseret tilgang og godt understøttet af årshjulet i FISKK og hver systemejer planlægger ledelsestilsynet på deres systemer og melder det ind via ServiceNow Socialforvaltningen vil udføre de manuelle ledelsestilsyn vedr. systemer udenfor IGA-løsningen hver 6. mdr. i overensstemmelse med kommunens regler herfor. SOF vil bestræbe sig på at placere forvaltningens egne ledelsestilsyn i de samme to årlige rul, dvs. omkring uge 9/10 og uge 37/38. Der kan dog være særlige forvaltningsspecifikke hensyn i SOF, der gør, at ledelsestilsynet må placeres på andre tidspunkter i løbet af året. • For de systemer, der ikke ligger i IGA-platformen, laves der et manuelt tilsyn og dokumentationen lægges i eDoc. Opgaven er løbende Deadline for samlet handleplan afhænger af KIT´s tilbagemelding.	**Socialforvaltningen** Ved næste opfølgning i juni 2024 vil Socialforvaltningen følge op på, at: 1. Tidshorisonten for KIT´s indsatser er kendt og følges. 2. KIT har leveret nogle bedre beskrivelser af roller og ensartet autorisationer, og at ledelsestilsyn bliver startet automatisk, hvilket vil være en stor hjælp for SOF og succesraten for gennemførte ledelsestilsyn. 3. KIT sammen med SOF har lagt en plan for migrering af evt. systemer, der endnu ikke er i IGA platformen. 4. Der er udført de planlagte ledelsestilsyn i uge 9/10. 5. Der er udført de planlagte manuelle ledelsestilsyn for de systemer der ikke ligger i IGA-platformen.
Sundheds- og Omsorgsforvaltningen I tilknytning til systemejerårshjulet for systemer, udarbejdes der to forvaltningsspecifikke arbejdsgange for gennemførsel af ledelsestilsyn med autorisationer. Arbejdsgangene vil omhandle hhv. ledelsestilsyn gennem IGA og tilsyn på systemer der endnu ikke er på IGA.	**Sundheds- og Omsorgsforvaltningen** SUF's Systemteam vil have gennemført ledelsestilsyn med autorisationer ud fra en risikobaseret tilgang, og oversigten over systemer.

Der udarbejdes en oversigt over senest gennemførte ledelsestilsyn vedr. SUF's systemer. Ledelsestilsyn prioriteres ud fra risikobaseret tilgang (systemets kritikalitet, antal brugere og mængden af personoplysninger). Ledelsestilsyn på systemer, der ikke er IGA-styret, vil som udgangspunkt, blive gennemført hver 6. måned, fsva. systemer indeholdende personoplysninger. De af forvaltningens systemer, der kan integreres i kommunens IGA-løsning, er blevet integreret. Ved nyanskaffelser stilles der krav om, at systemer skal kunne integreres i IGA. Af revisionens oversigt fremgår det at systemet TeleKOL (FISKK #3454) ikke har overholdt fristen for ledelsestilsyn. Systemet er ibrugtaget i marts 2023, og da det er IGA-styret skal ledelsestilsyn gennemføres årligt, dvs. senest marts 2024. Dette fremgår også af systemets årshjul.	Forvaltningsspecifikke arbejdsgange for ledelsestilsyn vil være udarbejdet og implementeret.
Teknik- og Miljøforvaltningen Forvaltningen har i løbet af de seneste to år haft fokus på ledelsestilsyn med brugerautorisationer. Forvaltningen har udarbejdet et årshjul, hvori ledelsestilsyn med brugerautorisationer både uden for og i IGA-løsningen indgår. Forvaltningen vil fortsat have fokus på at få de relevante fagsystemer migreret over på IGA-løsningen for at sikre en mere smidig ledelsestilsynsproces og bedre brugerstyring. Forvaltningen har besluttet en handleplan med tre indsatsområder, som forventes at være i overensstemmelse med fælles aktiviteter koordineret af ØKF: 1. Udførelse af ledelsestilsyn for systemer i IGA-løsningen, som følger forvaltningens årshjul (Q2 2024). 2. Udførelse af ledelsestilsyn for fagsystemer uden for IGA-løsningen (Q2 2024). 3. Udarbejdelse af plan for migrering af relevante systemer til IGA-løsningen i samarbejde med Koncern IT (Q3 2024)	**Teknik- og Miljøforvaltningen** Ved næste opfølgning i juni 2024 vil TMF følge op på at: 1. De planlagte ledelsestilsyn for systemer i IGA-løsningen er gennemført efter forvaltningens årshjul. 2. De planlagte ledelsestilsyn for fagsystemer uden for IGA-løsningen er gennemført. 3. Planen for migrering af relevante systemer til IGA-løsningen er udarbejdet.
Økonomiforvaltningen Økonomiforvaltningen har i egen forvaltning i 2023 haft fokus på kravene til ledelsestilsyn med autorisationer gennem bl.a. faste statusmøder og nyhedsbreve målrettet de it-systemansvarlige. IGA-integration af Økonomiforvaltningens it-systemer har ligeledes været et særligt fokusområde, hvorfor en stor andel af forvaltningens it-systemer er onboardet i løsningen. I forlængelse af ovenstående vil Økonomiforvaltningen i egen forvaltning gennemføre følgende tiltag. *Pkt. 1* Gennemgang af it-systemporteføljen i Økonomiforvaltningen med sikring af, at gennemførsel af tilsyn sker i overensstemmelse med kommunens regler.	**Økonomiforvaltningen** *Ad 1* Gennemgang af it-systemporteføljen i Økonomiforvaltningen foretages i Q1-2 2024 mhp. at identificere it-systemer, der mangler at gennemføre ledelsestilsyn med autorisationer. Tilsynene igangsættes løbende, så alle relevante tilsyn er gennemført inden udgangen af Q4 2024 og der er igangsat planlægning af relevante tilsyn for 2025. Større it-systemer, hvor ansvaret er placeret i Økonomiforvaltningen, med mange brugere på tværs af kommunen tilføjes Økonomiforvaltningens årshjul for gennemførelse af ledelsestilsyn. Der fortsættes med statusmøder mhp. opfølgning på implementering.

Pkt. 2 Gennemgang af, om der er yderligere systemer i Økonomiforvaltningen, der kan være relevante at onboarde på IGA og migrering af disse. **Deadline** Q4 2024	*Ad 2* Gennemgangen vil ske i løbet af Q1-2 2024 mhp. eventuel migrering af yderligere af Økonomiforvaltningens it-systemer inden årets udgang.

3.2.1 Ibrugtagning af it-systemer	
Farvemarkering (prioritet)	Rød
Gives til	Økonomiforvaltningen

Observationer og risici:
Observationen er foretaget af Deloitte, der på tidspunktet for konstateringen var kommunens eksterne revision.

Af forretningscirkulæret for it-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt it-system skal sikkerhedsvurderes, inden det idriftsættes.

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.

Det er forbundet med stor risiko for kommunen at idriftsætte et it-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse.

Forvaltningernes gennemgang viste, at der ultimo 2022 var 96 idriftsatte systemer anskaffet efter den 1. november 2018, uden en ibrugtagningstilladelse. Dette tal er efterfølgende justeret til 95 systemer.

Status 2023
De systemer, der blev identificeret i forbindelse med revisionsbemærkningen i 2022, er alle håndteret. Status den 30. oktober 2023 er

Status	**Antal**
Ibrugtagningstilladelse m. handleplan	41
Godkendt	17
Skal sikkerhedsvurderes ved væsentlige ændringer	17
Ikke godkendt	1
Udfaset	17
Planlagt udfaset	2
Total	**95**

Koncern-IT har oplyst, systemer ibrugtaget før 2018 skal først sikkerhedsvurderes, hvis der sker væsentlige ændringer. 17 systemer er derfor blevet undtaget sikkerhedsvurderingen.

Intern Revision har udtaget enkelte stikprøver med henblik på at undersøge, om der er sket ændringer til systemerne.

I to tilfælde var oplysningerne i FISKK ikke korrekte. Systemerne er først blevet registeret i henholdsvis 2020 og 2021.

I to tilfælde have systemet fået nye systemintegrationer, som jf. forretningscirkulæret for it-anskaffelser er en væsentlig ændring. Dette burde derfor have givet anledning til en sikkerhedsvurdering.
Der er 135 systemer, som er anskaffet før 1.november 2018, der ikke har en ibrugtagningsstatus.

Det er desuden konstateret, at der er 16 systemer, der har en "ikke godkendt" status. Systemerne ser forsat ud til at være i drift.

Et system har været i drift siden 2011, mens de øvrige er taget i drift i perioden 2014-2018.

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

Det henstilles at de systemer der ikke har en ibrugtagningsstatus, bliver gennemgået og oplysningerne i FISKK bliver opdateret. Det henstilles desuden, at der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018, som ifølge det oplyste først sikkerhedsvurderes, hvis der sker væsentlige ændringer. Umiddelbart er det vores vurdering at risikoen alt andet lige er større på ældre systemer. Det henstilles, at 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

Handleplan januar 2024	Opfølgning
Økonomiforvaltningen *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 (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 KIT i samarbejde med de givne forvaltninger vurderer det konkrete behov ud fra systemets kritikalitet set ift. de implementerede tekniske foranstaltninger. *Pkt. 3* I samarbejde med de systemansvarlige i forvaltningerne vil Koncern IT gennemføre den tilpassede sikkerhedsvurdering af de it-systemer, forvaltningerne melder ind 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. **<u>Deadline</u>** Det er forventningen, at arbejdet kan være gennemført mellem Q4 2024 og Q2 2025 afhængigt af den volumen af systemer, forvaltningerne indmelder til sikkerhedsvurdering som følge af deres gennemgang af systemporteføljen.	**Økonomiforvaltningen** *Ad 1* Koncern IT vil foreslå Digitaliseringschefkredsen, at der fastlægges deadline for opdatering af FISKK med udgangen af Q2 2024. Herefter følger Koncern IT op med fornyet sag til kredsen om status og evt. udeståender Q3 2024. *Ad 2* Koncern IT forelægger Digitaliseringschefkredsen en sag herom i Q2. *Ad 3* Koncern IT gennemgår forvaltningernes indmeldelser og påbegynder vurderingsarbejdet, som forventes afsluttet Q4 2024, men afhængigt af volumen, kompleksiteten af systemer, kompetencer og ressourcer i forvaltningerne kan pågå frem til Q2 2025. Digitaliseringschefkredsen og It-kredsen orienteres løbende om arbejdet, og Koncern IT vil eskalere eventuelle problemsager og kritiske sårbarheder, jf. gældende regler. *Ad 4* Gennemgangen vil ske i Q1 2024 og afklaring af nødvendig handling pr. it-system forventes at foregå frem til Q2 2024. It-kredsen vil blive forelagt eventuelle eskalationer for it-systemer, der ikke umiddelbart kan sikkerhedsvurderes eller godkendes løbende. Afhængigt af udfaldet af gennemgangen, herunder evt. behov for nye sikkerhedsvurderinger, forventes aktiviteten at være gennemført Q3 2024.

3.2.2 Organisering af informationssikkerhed og styrkelse af det ISMS	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen

Observationer og risici:
Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System).

Observationen er foretaget af Deloitte, der på tidspunktet var kommunens ekstern revision.

På baggrund af de konstant stigende trusler på informationssikkerhedsområdet er der behov for løbende at vurdere tilstrækkeligheden af de etablerede sikringsforanstaltninger, herunder sikre, at der er et ledelsessystem med tilstrækkelige kompetencer, ressourcer og uafhængighed på informationssikkerhedsområdet.

KK har nedsat et projekt med tilknyttet styregruppe, der har til formål at sikre et styrket ISMS.

Dette omfatter blandt andet forbedring af risikovurderinger, implementering af relevante sikringsforanstaltninger og rapportering på informationssikkerhedsområdet. Yderligere vil organisering af informationssikkerhedsområdet ligeledes blive vurderet, herunder sikre passende ressourcer med de nødvendige kompetencer og den nødvendige uafhængighed til at overvåge informationssikkerheden.

Status 2023
Der er blevet udarbejdet en GAP-analyse med henblik på at identificere mere specifikt, hvilke områder der skal styrkes.

Der er desuden blevet nedsat en styregruppe og oprettet en projektorganisering, der skal håndtere processen i forhold til at styrke kommunens ISMS og håndtere de observationer, der er påpeget i GAP-analysen.

Det er aftalt med ledelsen i KIT, at observationen omkring leverandørstyring indgår som en del af kommunes fremtidige ISMS, hvorfor observationen er indarbejdet i dette punkt, hvor følgende risiko blev noteret: ”Manglende eller utilstrækkelig styring og monitorering af leverandører medfører risiko for, at de leverede ydelser ikke dækker forretningsmæssige behov, samt at leverandører ikke efterlever det forventede IT-sikkerhedsniveau.”

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller, at arbejdet med at styrke informationssikkerheden fortsat prioriteres højt, herunder at: ► Der med afsæt i den foretagne GAP-analyse identificeres, hvilke områder der skal styrkes ► Det vurderes, hvorledes organiseringen af informationssikkerhedsområdet bør være, så dette sikrer tilstrækkelige kompetencer og uafhængighed. Der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt. Vi henstiller, at der etableres en proces for opfølgning på leverandører som omfatter en risikovurdering af leverandøren og de services der leveres og på baggrund heraf og at der foretages en stillingtagen om hvorledes overvågningen af leverandøren skal foretages, eks. ► Modtagelse af erklæring ► SLA rapportering ► Møder med leverandør ► Spørgeskemaer til leverandør El.lign.	Økonomiforvaltningen

Handleplan januar 2024	Opfølgning
Økonomiforvaltningen *Pkt. 1*	**Økonomiforvaltningen** *Ad 1-3*

Cyber- og informationssikkerhedsprogrammet arbejder i 2024 på at udvikle og implementere et koncernfælles Informationssikkerhedsledelsessystem (ISMS) på tværs af alle forvaltninger. Der er fokus på at styrke arbejdet med Enterprise Risk Management, herunder at implementere kontroller fra både ISO 27001 og de kommende krav fra EU-direktivet 'NIS2'. *Pkt. 2* Cyber- og informationssikkerhedsprogrammet vil udarbejde et beslutningsoplæg til den fremadrettede organisering for arbejdet med ISMS i KK, herunder kontrol og tilsyn med de iværksatte sikringstiltag og tilhørende ledelsesrapportering. KIT har igangsat en afprøvning af det samlede ISMS koncept på et udvalgt forretningskritisk område. Afprøvningen forventes afsluttet i Q2 2024, og skal benyttes som afsæt for implementering af det samlede ISMS. Den endelige implementering og konsolidering af et koncernfælles ISMS i forvaltningerne forventes at strække sig til slutningen af 2025 og herefter overgå til løbende drift og videreudvikling, herunder ift. eventuel systemunderstøttelse. *Pkt. 3* Økonomiforvaltningen vil indarbejde vurdering af leverandører i risikovurdering af it-systemer, så der ifm. vurderingen tages stilling til risiko for 3. parts it-systemer. På baggrund af vurderingen af risici, vil der blive anbefalet foranstaltninger, man som systemejer bør tage, herunder fx indhente revisorerklæring, SLA rapportering, møder med leverandøren, spørgeskemaer til leverandøren mv. **Deadline** Q4 2025	Opfølgningen vil ske i regi af Cyber- og informationssikkerhedsprogrammets styregruppe. Organisering for arbejdet med ISMS i KK forventes at være besluttet Q2 2024 mhp. at blive implementeret i Q3 og Q4. Det efterfølgende arbejde og implementering af ISMS koordineres ligeledes gennem styregruppen og It-kredsen, der løbende vil blive forelagt sager, jf. den organisering der besluttes. Det forventes, at selve implementeringen med efterfølgende dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt vil foregå i 2025.

3.2.3 Risikovurderinger	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen
Observationer og risici: Observationen er foretaget af Deloitte, der på tidspunktet var kommunens ekstern revision. Risikovurderinger af systemer foretages ikke for alle systemer, men kun de systemer, der enten har været i drift i minimum fire år, eller hvor forvaltningen er usikker på, om informationssikkerhedsniveauet er tilstrækkeligt, samt for systemer, der anvendes tværgående i KK's forvaltninger. I forhold til de foretagne risikovurderinger har Deloitte noteret, at disse er baseret på en liste af "standard" kontrolområder. Der ligger ikke et egentlig opdateret trusselskatalog til grund for disse risikovurderinger. Ligeledes kunne de ikke, på baggrund af den foreliggende dokumentation, se, at der er konsekvent, der foretages en dokumenteret vurdering af, hvorvidt de mitigerende sikringstiltag og kontroller faktisk fungerer hensigtsmæssigt. **Status 2023** Der arbejdes fortsat på et nyt risikovurderingskoncept baseret på egentligt trusselskatalog.	
Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller, at:	Økonomiforvaltningen

▶ De nuværende risikovurderinger af systemer styrkes, så det sikres, at alle relevante systemer bliver omfattet og med afsæt i opdaterede trusselsvurderinger ▶ Der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt ▶ Der udarbejdes en plan, der viser, hvor mange systemer, der fremover risikovurderes, og hvor tit det vil blive foretaget. Planen bør ligeledes omfatte et overblik over det efterslæb, som der er pt.	

Handleplan januar 2024	Opfølgning
Økonomiforvaltningen *Pkt. 1* For at imødegå bemærkningen fra Deloitte fra 2022 har KK igangsat et arbejde med at implementere et nyt risikovurderingskoncept, der gør brug af et trusselskatalog, som vedligeholdes i Koncern IT. Konceptet blev, jf. handleplan for 2022 bemærkningen, udarbejdet i 2023 mhp. implementering i 2024 og vil medføre, at KK vil risikovurdere it-systemer i drift i et omfang og en frekvens, der fastsættes på baggrund af it-systemernes individuelle kritikalitet og restrisici. Udviklingsarbejdet er baseret på en agil metode med iterative fremskridt baseret på de erfaringer, projektet og interessenterne gør sig, hvorfor relevante kredse løbende inddrages ift. godkendelse. *Pkt. 2* Arbejdet med det nye risikovurderingskoncept har snitflader og afhængigheder til ISMS-implementeringen, herunder ift. opfølgning på etablerede sikringstiltag og kontroller for forvaltningernes kritiske forretningsprocesser, som strækker sig ind i 2025, jf. handleplanen for ISMS. Koncern IT er ansvarlige for begge aktiviteter og vil sikre sammenhængen mellem dem. *Pkt. 3* KK vil fremover risikovurdere it-systemer i drift i et omfang og en frekvens, der fastsættes på baggrund af systemernes individuelle kritikalitet og restrisici. Koncern IT vil i samarbejde med Digitaliseringschefkredsen udarbejde en opdateret plan for de løbende risikovurderinger. Da revisionsbemærkningen vedr. ibrugtagningstilladelser ligeledes indebærer sikkerhedsvurderinger af it-systemer med stillingtagen til risiko, vil arbejdet med de løbende risikovurderinger ske ud fra et hensyn til gennemførelse af denne handleplan. **Deadline** Q2 2025	**Økonomiforvaltningen** *Ad 1* Arbejdet koordineres med forvaltningerne gennem Digitaliseringschefkredsen og It-kredsen, som vil blive forelagt en sag om godkendelse af det nye risikovurderingskoncept i Q2 og løbende blive inddraget i trit med at modellen videreudvikles. *Ad 2* Arbejde med styring af forvaltningernes kritiske forretningsprocesser i KK's ISMS forventes at strække sig ind i 2025. Proces for arbejdet er beskrevet i handleplanen for ISMS. *Ad 3* Planen for arbejdet med løbende risikovurderinger forventes færdig og forelægges Digitaliseringschefkredsen og It-kredsen til godkendelse Q3 2024. Planen tilrettelægges med hensyn til gennemførelse af handleplan for revisionsbemærkningen vedr. ibrugtagningstilladelser, som forventes at medføre en stor mængde sikkerhedsvurderinger, der skal gennemføres inden arbejdet med de løbende risikovurderinger kan sættes fuldt i drift. Afhængigt af antal, volumen og kompleksitet af de systemer, der indmeldes til sikkerhedsvurdering som følge af denne handleplan, vil dette kunne strække sig til Q2 2025.