Handleplaner til revisionsbemærkninger vedrørende årsregnskabet 2024 og opfølgning på handleplaner fra den løbende revision 2024

Revisionsbemærkninger rapporteret i løbet af året	
Nr. 1 Ibrugtagningstilladelser på it-systemer	Forvaltningerne
Revisionsbemærkninger vedrørende årsregnskabet	
Nr. 2 Forsikring ØKF	Økonomiforvaltningen
Nr. 3 Informationssikkerhed	Forvaltningerne
Nr. 4 Ejendomsvedligehold	Økonomiforvaltningen
Nr. 5 Fritagelse for ejendomsskat	Økonomiforvaltningen
Nr. 6 Godkendelse af indkøb BUF	Børne- og Ungdomsforvaltningen
Nr. 7 Revision af balancen	Forvaltningerne
Nr. 8 Anlægsprojekter	Teknik- og Miljøforvaltningen, Økonomiforvaltningen, Socialforvaltningen, Kultur- og Fritidsforvaltningen, Beskæftigelses- og Integrationsforvaltningen
Nr. 9 Egenbetaling – Indtægter SOF	Socialforvaltningen

Handleplan august 2025 - vejledning	**Opfølgningsplan / Status august 2025**
Handleplan *Handleplanen skal forholde sig til alle de konkrete observationer i revisionsbemærkningen.* *Angiv handleplan i punktform med konkrete tiltag for at håndtere problemstillingen. Alle tiltag skal være tidsfastsat ift. forventet dato for gennemførsel.* *Handleplanerne skal:* • *Identificere problemet/problemstillingen* • *Beskrive omfanget af problemet* • *Beskrive tiltagene for at løbe problemet – og forholde sig til alle dele af det konkrete indhold i bemærkningen. Dette skal være med et fremadrettet sigte.* • *Anføre, hvornår forholdene forventes at være berigtiget og klar til revision. Der skal være deadlines for, hvornår de enkelte delaktiviteter og den samlede handleplan forventes afsluttet.* • *Angive, hvornår der følges op på om de besluttede tiltag virker efter hensigten.* *Derudover skal handleplanerne:* • *Være forståelige, de skal være til at forstå for politikere, ministeriet eller andre, der ikke har et indgående kendskab til fagområdet.* • *Være skrevet i punktform, således der for hvert punkt i handleplanen kan udarbejdes et opfølgningspunkt, der beskriver, hvordan forvaltningen vil følge op på, om de konkrete handleplaner har resulteret i en forandring, når handleplanen er gennemført.* ***Deadline for samlet handleplan:*** *Angivelse af den samlede deadline for håndtering af revisionsbemærkningen.*	***Ved udarbejdelse af handleplan*** *Her skal der for hvert punkt i handleplanen angives, hvordan forvaltningen vil følge op på, om de konkrete handleplaner har resulteret i en forandring, når handleplanen er gennemført.* ***Opfølgning*** *For hvert punkt i handleplanen skal der* 1. *enten gives en status for handleplanen. Hvis der er forsinkelser, skal årsagen til forsinkelsen angives, samt den opdaterede forventede gennemførselsdato skal angives, eller* 2. *Beskrives, hvad den opfølgende egenkontrol har resulteret i, hvis handleplanen er afsluttet.*

Handleplan august 2025 - vejledning	Opfølgningsplan / Status august 2025

Nr. 1 Ibrugtagningstilladelser på it-systemer	
Gives til	Forvaltningen

Observationer og risici:

Af Forretningscirkulæret for it-anskaffelser, der er bindende for alle forvaltninger, fremgår det, at et nyt it-system skal sikkerhedsvurderes og have en ibrugtagningstilladelse, inden det idriftsættes. En sikkerhedsvurdering tager stilling til, at alle krav til informationssikkerhed og databeskyttelse er opfyldt. Hvis en ibrugtagningstilladelse ikke kan udstedes forud for idriftsættelsen, skal sagen behandles som uoverensstemmelse. Dette indebærer en eskalering til relevante ledelsesforaer, hvor der skal opnås enighed, hvis sagen ikke skal eskaleres yderligere til de relevante administrerende direktører, borgmestre og ultimativt til Økonomiudvalget. Det er forbundet med stor risiko for kommunen at idriftsætte et it-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse.

Opfølgning 2024

Forvaltningernes har besluttet og igangsat en handleplan, som omfatter:

1. KIT foretager en tilpasset sikkerhedsvurdering af
   - IT-systemer i drift fra før 2018, der har undergået væsentlige ændringer.
   - 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):**
I lighed med tidligere år henstilles det, at - at der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018, samt, - 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.	Forvaltningerne

Handleplan august 2025	Status august 2025
Børne- og Ungdomsforvaltningen 1.Gennemgang af ibrugtagningsstatus BUF ansætter en ressource til at varetage porteføljemanagement på IT-ressourcer. Systemerne uden ibrugtagningsstatus bliver gennemgået i 2024. 2.Tilpasset sikkerhedsvurdering BUF's porteføljemanager (ressourcen under punkt 1) er sammen med GDPR-funktionen og BUF's tekniske systemejer i gang med at gennemgå BUF's IT-portefølje. Der er særlig fokus på mindre decentrale systemer og systemer anskaffet før 2018. Porteføljemanagere og systemejere udarbejder parallelt med dette en kritikalitetsscoring af de systemer, der indgår i KIT's konsolideringsplan. På baggrund af kritikalitetsscoringen vil KIT igangsætte en risikovurdering af de berørte systemer.	**Børne- og Ungdomsforvaltningen** 1.BUF har indmeldt alle systemer, som mangler en ibrugtagningstilladelse. Der samarbejdes tæt med KIT om at sikre de sidste ibrugtagningstilladelser kommer i mål. 2.Systemporteføljen også systemer før 2018 er gennemgået i løbet af foråret 2025 og kritikalitetsscoringen er gennemført for projekterne. 3.Ny proces er etableret og alle relevante systemer er meldt ind til KIT mhp. ibrugtagningstilladelser.

3.Systemer med status "ikke godkendt" BUF skal lave de tilpassede sikkerhedsvurderinger. I samarbejde med KIT skal der udarbejdes de ibrugtagningstilladelser, der mangler. Det vedrører fortsat systemer før 2018. BUF vil forbedre indmeldelsen af nye systemer, man ønsker at anskaffe, så alle ønsker bliver godkendt i digitaliseringsafdelingen. Det skal sikre, at man ikke lokalt kan købe og ibrugtage et system uden de nødvendige sikkerhedsgodkendelser. Arbejdet med at lave en bedre proces vil foregå i 2024 og løbende revurderes.	

Nr. 3 Informationssikkerhed	
Gives til	Forvaltningerne

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.

ØKF har udarbejdet et dokument der beskriver hovedbestanddelene i en ISMS-implementering omfattende den samlede informationssikkerhed i Københavns Kommune:

1. Topledelsen beslutter overordnet organisering, risikovillighed, krav til rapportering mv., som ønskes. Beslutningen træffes ud fra det aktuelle trusselsniveau, kritikalitet af kerneopgaver og typer af data, som den ønsker.
2. ISMS'ets fundament i form af nødvendige styringsdokumenter udformes og godkendes af relevante instanser. Fundamentet kommunikeres gennem bl.a. skriftlige produkter, uddannelse og workshops.
3. Forretningsaktiviteter risikovurderes i forhold til informationssikkerhedsmæssige risici. Risici planlægges nedbragt til acceptabelt niveau gennem implementering af nødvendige foranstaltninger. Topledelsen inddrages i risikoaccept.
4. Konkrete organisatoriske, teknologiske, fysiske og menneskelige foranstaltninger implementeres ud fra kravgrundlag, standarder mv.
5. Compliance og dokumentationsarbejde samler op på identificerede risici, status for implementering af foranstaltninger, målopfyldelse mv. gennem bl.a. monitorering, (selv)evalueringer og revisioner. Der er i praksis en løbende vekselvirkning mellem nr. 3, 4 og 5. På baggrund heraf evalueres ISMS'et med rapportering og anbefalinger til topledelsen.
6. Topledelsen beslutter på baggrund af rapportering, om ISMS'et er egnet, tilstrækkeligt og effektivt, og hvilken videre udvikling arbejdet skal fortsætte i. Herefter returneres til punkt 1 eller 2.

Når ISMS'et er etableret, skal cyklussen køre på hhv. KK-niveau og på forvaltningsniveau.

Det er således forventningen, at der i hver af de syv forvaltninger kører parallelle rapporterings- og beslutningsprocesser mod egen direktion, og at Økonomiforvaltningen på den baggrund herfra sammenstiller en overordnet rapportering og status til ØU.

I tillæg hertil arbejdes med supplerende handleplaner som i væsentlig grad er væsentlige og nødvendige tiltag i forhold til informationssikkerheden i KK.

- Implementering af CIS 18 kontroller på cybersikkerhedsområdet inden for den it-infrastruktur, som Økonomiforvaltningen varetager
- Ændring af IT-Anskaffelsesprocessen

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
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. 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. Det henstilles endvidere, at: ▶ implementering af CIS 18 kontroller på cybersikkerheds- området sker hurtigst muligt og omfatter den samlede it-infrastruktur i KK ▶ it-anskaffelsesprocessen følger de krav der stilles i ISO'erne, herunder 27001 Anneks A. Anneks A omhandler de sikkerhedskontroller, som KK bør implementere i forbindelse med en it-anskaffelsesproces der skal sikre en sammenhængende informationssikkerhed i KK baseret på standarder og best practice.	Forvaltningerne

Handleplan august 2025	**Opfølgningsplan**
Tværgående handleplan Handleplanen består af tre delelementer, som beskrives nedenfor: 1) ISMS, 2) Implementering af CIS18-kontroller, 3) It-anskaffelsesprocessen. <u>1. ISMS</u> Implementeringen af et ISMS i KK følger den vedtagne handleplan som beskrevet i revisionsbemærkningen. Arbejdet ledes af CISO-funktionen i ØKF, og der er ved at blive 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. <u>2. Implementering af CIS18-kontroller</u> 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.	**Tværgående** <u>1. ISMS</u> Fase 1 forløber frem til marts 2026, hvor der foretages et 'stop and go' med beslutning om næste fase i IT-kredsen. IT-kredsen er styregruppe for ISMS implementeringen og vil løbende få forelagt og tage stilling til fremdriften. <u>2. Implementering af CIS18 kontroller</u> ØKF nedsætter en arbejdsgruppe på tværs af forvaltninger mhp. at løse punkt A og B. Resultaterne forelægges eksisterende kredse mhp. ITK kan træffe beslutning om de to punkter. Som en del af governancen for brug af CIS18-kontroller og etableringen af det samlede ISMS for KK følges op på den ønskede forandring. <u>3. IT-anskaffelsesprocessen følger ISO-krav</u> I forbindelse med en ny it-anskaffelsesmodel opdateres eksisterende forretningsgange, hvoraf det vil fremgå, hvem der har ansvar for hvad for at sikre overholdelse af kravene. Det vil ligeledes kunne indgå i ISMS rapporteringen, men niveauet herfor er ikke fastlagt endnu, så der er ikke taget stilling hertil.

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 handleplaner 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. Det bemærkes, at det i aftalen om kommunernes økonomi for 2026 er aftalt, at kommunerne pr. 1. januar 2027 skal etablere 4-5 nye IT-serviceorganisationer for at samle og effektivisere den basale IT-drift. Udfoldelsen og implementeringen heraf kan influere på, hvor det er mest givtigt for KK at lægge fokus i implementering af CIS18. <u>3. IT-anskaffelsesprocessen følger ISO-krav</u> 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.	

Nr. 6 Godkendelse af indkøb BUF	
Gives til	Børne- og Ungdomsforvaltningen
Observationer og risici: Jævnfør kommunens regler skal det i forbindelse med indkøb af varer og tjenesteydelser godkendes, at varen/ydelsen er bestilt/modtaget og svarer til det aftalte (varemodtagelse) forinden fakturaen ledelsesgodkendes og betales.	

Kontrollen skal som hovedregel udføres af en person med tilstrækkelig viden om indkøbet, hvilket typisk vil være indkøberen/bestilleren. I BUF anvendes "stedfortræderrollen" i mange tilfælde til formel godkendelse i Kvantum og som oftest foretages varemodtagegodkendelsen uden tilstrækkelig viden om indkøbet.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Kontrolmiljøet er i strid med det af Økonomiudvalget godkendte "Forretningscirkulære Indkøb", som foreskriver en forebyggende varemodtagelseskontrol forinden fakturaen godkendes og betales. Vi henstiller, at BUF ► følger kommunens vedtagne regler om varemodtagelse, så det er dokumenteret, at alle indkøb er godkendt af personer med tilstrækkelig viden om, at varen/ydelsen er bestilt/modtaget og svarer til det aftalte, ► anvender "stedfortræderrollen" i Kvantum i overensstemmelse med de beslutninger, der er truffet i KK (linjeledelsesprincippet).	Børne- og Ungdomsforvaltningen

Handleplan august 2025	**Opfølgningsplan**
Børne- og Ungdomsforvaltningen Forvaltningen har flere initiativer i gang for at sikre varemodtagelse. 1. Forvaltningen vil ændre EAN-strukturen, så hver enhed for sit eget EAN-nummer. Dette skal resultere i en øget brug af Let-betaling. Der er ca. 700 enheder der skal have ændret EAN og efterfølgende informeres leverandørerne. Målet er at optimere ressourcerne på controlling og varemodtagelse. Implementeringen er startet op i 2. kvartal 2025 og der forventes at strukturen er på plads ved årets udgang. 2. Flere Indkøb gennem Kvantum: Der igangsat en evaluering af den indsats, der hidtil er foretaget for at flere indkøb til at foregå via indkøbsløsningen i Kvantum. Evalueringen laves med henblik på at identificere uudnyttede potentialer, der kan styrke indkøbsprocedurerne. Baseret på resultaterne af evalueringen, vil indsatsen blive justeret. 3. Gennemgang af roller og rettigheder i Kvantum: Forvaltningen er i gang med en systematisk gennemgang af roller og rettigheder i Kvantum. Målet er at optimere stedfortræderordninger baseret på risikovurderinger og få beskrevet processen omkring tildeling af roller og rettigheder. 4. I forlængelse af ovenstående punkter har forvaltningen foretaget en analyse og vurdering af, om der kan foretages ændringer i kommunens regler, så disse understøtter, at der kan etableres ressourceeffektive og betryggende processer i administrative fællesskaber i relation til varemodtagelse og fakturagodkendelse. Forvaltningen er i dialog med ØKF og øvrige forvaltninger omkring afdækning af mulighederne for en ændret model.	**Børne- og Ungdomsforvaltningen** 1.Overvågning af EAN-implementering: Overvågning af implementeringen hver måned fra 2. kvartal 2025 til udgangen af året. 2.Evaluering af Indkøb gennem Kvantum: Udmøntning af justeringsplanen baseret på evalueringsresultater i 4. kvartal 2025. Planlagte opdateringer til implementering med deadline i 1. kvartal 2026. 3.Gennemgang af roller og rettigheder i Kvantum: Forventes færdiggjort inden udgangen af 4. kvartal 2025. 4.Dialog om ændringer i kommunens regler: ØKF har modtaget vores udkast til en ændring af forretningsområdet og vi afventer tilbagemelding ultimo 2. kvartal 2025.