ØKF Kontor for Økonomistyring og Regnskab (2391)
Økonomiforvaltningen

Cover

Til Økonomiudvalget

Orientering om den løbende revision 2024

07-01-2025

Sagsnummer i F2
2024 - 25488

Dokumentnummer i F2
6900748

Sagsnummer eDoc
2024-0428345

Resumé
Københavns Kommune har i henhold til normal praksis modtaget de tre revisionsrapporter, der indgår i den løbende revision af Københavns Kommunes regnskab 2024. Der er i de tre rapporter givet ni røde bemærkninger (prioritet 1), hvoraf seks er nye i forhold til 2023, og tre er videreførte. Der lukkes med rapporterne to røde bemærkninger.

Idet alle rapporter indeholder røde revisionsbemærkninger, skal Økonomiudvalget orienteres herom senest tre uger efter, at Økonomiforvaltningen har modtaget revisionsrapporterne fra revisionen. Økonomiudvalgets behandling af rapporterne vil ske på mødet den 25. februar 2025. På samme møde vil handleplaner til de enkelte bemærkninger, som forvaltninger udarbejder, blive forelagt.

Sagsfremstilling
Københavns Kommune har i december 2024 modtaget revisionsrapporterne for den løbende revision 2024, som består af tre rapporter:

- Regnskabsføring, forretningsgange og interne kontroller 2024
- Revision af generelle IT-kontroller 2024
- Revision af løn- og personaleområdet 2024

<u>Regnskabsføring, forretningsgange og interne kontroller 2024</u>
Med rapporten afgiver revisionen to røde (prioritet 1) revisionsbemærkninger. De to bemærkninger vedrører 'Administration af autorisationer til Kvantum' og 'Brugeradministration Kvantum (SAP Basis)', hvor førstnævnte er en ny bemærkning og sidstnævnte er videreført fra 2023. Begge bemærkninger vedrører samme tematik om, at der er brugere, som har kritiske rettigheder til produktionsmiljøet i Københavns Kommunes økonomisystem, Kvantum.

Derudover er der afgivet tre gule (prioritet 2) og to grønne (prioritet 3) bemærkninger. To af de gule bemærkninger (Administration af autorisationer Kvantum og Bilagskontrol) har ændret farve fra at være røde i 2023 til at være gule i 2024. En grøn bemærkning (Bilagskontrol) har ligeledes ændret farve fra rød i 2023 til at være grøn i 2024.

Der lukkes to røde og to gule revisionsbemærkninger med rapporten. Rapporten er vedlagt, som bilag 1.

Af tabel 1 fremgår revisionsbemærkningerne givet i rapporten om Regnskabsføring, forretningsgange og interne kontroller 2024, samt hvilke forvaltninger, der har fået bemærkningen.

Tabel 1. Revisionsbemærkninger i Regnskabsføring, forretningsgange og interne kontroller 2024

Regnskabsføring, forretningsgange og interne kontroller 2024	
3.1.1.1 Administration af autorisationer til Kvantum (rød) (ny)	Økonomiforvaltningen
3.1.1.2 Administration af autorisationer til Kvantum (gul) (ny)	Økonomiforvaltningen
3.1.2.1 Bilagskontrol (gul) (var rød i 2023)	Børne- og Ungdomsforvaltningen, Socialforvaltningen
3.1.2.2 Bilagskontrol (grøn) (var rød i 2023)	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

Revision af generelle IT-kontroller 2024

Med rapporten afgiver revisionen seks røde (prioritet 1) bemærkninger, hvoraf fire er nye (Organisering af informationssikkerhed og styrkelse af ISMS, Risikovurderinger af it-systemer, Åbning af det produktive miljø (Kvantum) og Log af åbninger (Kvantum)), og to er videreførte fra 2023 (Ledelsestilsyn med bruger autorisationer og Sikkerhedsvurdering af systemer). To af de nye røde bemærkninger (Organisering af informationssikkerhed og styrkelse af ISMS og Risikovurderinger af it-systemer) var gule bemærkninger i 2023, men de har ændret karakter i den løbende revision 2024.

Desuden gives der to gule (prioritet 2) bemærkninger med rapporten.

Der lukkes ikke revisionsbemærkninger med rapporten. Rapporten er vedlagt, som bilag 2.

Af tabel 2 fremgår revisionsbemærkningerne givet i rapporten om Revision af generelle IT-kontroller 2024, samt hvilke forvaltninger, der har fået bemærkningen.

Tabel 2. Revision af generelle IT-kontroller 2024

Revision af generelle IT-kontroller 2024	
3.1.1 Organisering af informationssikkerhed og styrkelse af ISMS (rød) (ny rød – var gul i 2023)	Økonomiforvaltningen
3.2.3 Risikovurderinger af it-systemer (rød) (ny rød – var gul i 2023)	Økonomiforvaltningen
3.1.3 Åbning af det produktive miljø (Kvantum) (rød) (ny)	Økonomiforvaltningen
3.1.4 Log af åbninger (Kvantum) (rød) (ny)	Økonomiforvaltningen
3.1.5 Password opsætning (Kvantum) (gul) (ny)	Økonomiforvaltningen
3.1.6 Gennemgang af rettigheder (Kvantum) (gul) (ny)	Økonomiforvaltningen
3.2.1 Ledelsestilsyn med bruger autorisationer (rød)	Forvaltningerne
3.2.2 Sikkerhedsvurdering af systemer (rød)	Forvaltningerne

Revision af løn- og personaleområdet 2024
Rapporten indeholder en rød (prioritet 1), en gul (prioritet 2) og to grønne (prioritet 3) bemærkninger. Alle bemærkninger er nye i 2024. Rapporten er vedlagt, som bilag 3.

Af tabel 3 fremgår revisionsbemærkningerne givet i rapporten om Revision af løn- og personaleområdet 2024, samt hvilke forvaltninger, der har fået bemærkningen.

Tabel 3. Revision af løn- og personaleområdet 2024

Revision af løn- og personaleområdet 2024	
4.4 Afregning til Feriefonden (rød) (ny)	Forvaltningerne
4.1 Arbejdsskade (gul) (ny)	Økonomiforvaltningen
4.3 Sagsgennemgang (grøn) (ny)	Økonomiforvaltningen
4.2 VIP-kontrol (grøn) (ny, lukket)	Økonomiforvaltningen

Økonomi
Sagen har ikke økonomiske konsekvenser.

Videre proces
Økonomiforvaltningen indhenter handleplaner til røde og gule bemærkninger fra de ansvarlige forvaltninger, som, i det omfang de vedrører andre forvaltninger end Økonomiforvaltningen, behandles på fagudvalgene i løbet af januar-februar 2025. Herefter forelægges Økonomiudvalget handleplanerne på mødet den 25. februar 2025.

Bilag
Bilag 1 – Regnskabsføring, forretningsgange og interne kontroller 2024
Bilag 2 – Revision af generelle IT-kontroller 2024
Bilag 3 – Revision af løn- og personaleområdet 2024

Københavns Kommune

Revisionsrapport – Regnskabsføring, forretningsgange og interne kontroller 2024

Økonomiforvaltningen
Att.: Adm. direktør Søren Hartmann Hede
Direktør Nicolai Kragh Petersen
Københavns Rådhus
1599 København V

Intern Revision

KØBENHAVNS KOMMUNE

EY
Building a better working world

1 Formål, omfang m.v.

Som led i den løbende revision af Københavns Kommunes regnskab for 2024 har vi foretaget revision af kommunens regnskabsføring, forretningsgange og interne kontroller generelt samt for indkøbsområdet.

Rapporten skal ses i sammenhæng med revisionsrapporten "Revision af generelle IT-kontroller 2024", hvor forhold relateret til de generelle IT-kontroller er opsummeret.

1.1 Revisionens formål

Revision af kommunens forretningsgange og interne kontroller er en del af den lovpligtige revision og indgår i grundlaget for vores påtegning af Københavns Kommunes årsregnskab. Revisionens formål er at undersøge, om området administreres betryggende og i overensstemmelse med borgerrepræsentationens beslutninger, gældende love og andre forskrifter samt med indgåede aftaler og sædvanlig praksis, endvidere at foretage en kritisk gennemgang af forretningsgange og de kontroller, der er etableret på området.

Det bedste værn mod uregelmæssigheder er hensigtsmæssige forretningsgange og gode interne kontroller, hvorfor vores revision i vidt omfang har baseret sig på efterprøvelse af forretningsgange og interne kontroller, men ikke undersøgelser specielt med henblik på opdagelse af uregelmæssigheder.

Det påhviler ledelsen at tilrettelægge kontrolsystemer og forretningsgange, der er betryggende efter forvaltningens forhold, og det påhviler revisor at gennemgå disse forretningsgange og interne kontroller, som et led i revisionen af årsregnskabet.

1.2 Revisionens omfang og afgrænsning

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for væsentlig fejl.

Det er ledelsens ansvar at tilrettelægge niveauet for hensigtsmæssige og betryggende interne kontroller i overensstemmelse med kommunens kasse- og regnskabsregulativ m.v.

Revisionen er baseret på en forventning om, at der er tilrettelagt et velfungerende internt kontrolsystem og en pålidelig bogføring. Dette indebærer, at det overordnede kontrolmiljø og de organisatoriske rammer understøtter et velfungerende ledelses- og kontrolsystem, og at der på de enkelte aktivitetsområder er beskrevet og implementeret interne kontroller, som reducerer risikoen for væsentlige fejl til et acceptabelt niveau.

Ud fra ovenstående har vi tilrettelagt vores løbende revision af regnskabsføring, forretningsgange og interne kontroller 2024.

I forbindelse med revisionen tester vi de interne kontroller, i det omfang vi finder det nødvendigt for revisionen af årsregnskabet. Revisionen omfatter ikke en gennemgang af samtlige bilag og transaktioner, men udføres ved, at vi ved stikprøver indhenter dokumentation for eller på anden måde får bekræftet bogføringens rigtighed.

Vi skal gøre opmærksom på, at revisionen først anses for afsluttet, når vi har underskrevet erklæringen på årsregnskabet.

1.3 Revisionsarbejdets udførelse

Revisionen omfatter Intern Revisions bistand til EY i forbindelse med lovpligtig revision af forretningsgange og de tilrettelagte kontroller på økonomiområdet. Revisionen er udført på grundlag af godkendt revisionsplan for 2024 og er blandt andet gennemført ved besøg hos Koncernservice (KS) og centralenheder i forvaltningerne.

Ved revisionen har vi vurderet de processer, der er væsentlige for revisionen af kommunens årsrapport.

Revisionen har omfattet vurdering af kontrollernes:

- **Design** – og hvorvidt der på de konkrete aktiviteter er identificeret risici, som kan medføre tilsigtede eller utilsigtede fejl og mangler, og om der er udarbejdet hensigtsmæssige og betryggende forretningsgange og interne kontroller, der afdækker disse.
- **Implementering** - og om de udarbejdede retningslinjer og interne kontroller rent faktisk er implementeret i kommunen.
- **Effektivitet** – og hvorvidt kontrollerne har fungeret efter hensigten og har medvirket til at forebygge eller opdage tilsigtede og utilsigtede fejl og mangler på de konkrete aktiviteter i hele regnskabsåret. Dette omfatter alene kontroller, som vurderes særlig afgørende for at sikre mod væsentlige fejl i forbindelse med kommunens regnskabsaflæggelse.

2 Ledelsesresumé og konklusion

I forbindelse med den løbende revision af regnskabsføring, forretningsgange og interne kontroller for 2024 har vi identificeret de processer, der er væsentlige for revisionen, og vurderet design og implementering af forretningsgange og interne kontroller. Hvor det bidrager til vores revisionsoverbevisning samt forståelse af kontrolmiljøet på området, har vi testet kontrollernes design, implementering og effektivitet.

På baggrund af vores gennemgang er det vores vurdering, at der generelt er etableret et godt kontrolmiljø.

Den tilbagevendende analyse af funktionsadskillelseskonflikter i Kvantum har i 2024 afdækket, at der i forbindelse med revisionen identificeres en generisk konto med fuld adgang til SAP Kvantum-applikationen. Derudover er der konstateret flere SoD-konflikter samt enkelte brugere med udvidede SAP Basis-roller. Vi henstiller til, at forholdene omkring SOD og rettigheder bliver håndteret og mitigeret.

I lighed med de foregående år har vi i 2024 haft særligt fokus på fyldestgørende og tilstrækkelig dokumentation for de regnskabsmæssige registreringer.

En forudsætning for at god regnskabsskik er efterlevet, og at kontrolmiljøet vedrørende betalinger er effektivt, er, at rekvirenten vedlægger tilstrækkelig dokumentation så 2.-godkender har adgang til et fyldestgørende regnskabsmateriale. Manglende dokumentation øger også risikoen for, at besvigelser kan holdes skjult, hvis det ikke er muligt at påse, hvilke ydelser m.v. fakturaen reelt dækker.

På tværs af kommunen er der generelt sket et løft af kontrolmiljøet relateret til dankort og udlæg, idet der i forvaltningerne, med fejl på området, udføres en central bilagskontrol. Vi har foretaget en re-performance af forvaltningernes bilagskontrol.

Overordnet kan forvaltningernes bilagskontrol opsummeres således:

- KFF og BIF vurderes i al væsentlighed at efterleve kravene vedrørende fyldestgørende og tilstrækkelig dokumentation for de regnskabsmæssige registreringer for dankort og udlæg samt at de har etableret et tilstrækkeligt kontrolmiljø for området.
- ØKF, SUF og TMF har etableret en stikprøvevis bilagskontrol, og der konstateres få fejl i de udvalgte registreringer. Dette bekræfter vores re-performance af kontrollen.
- SOF og BUF har udført den stikprøvevise bilagskontrol i 2024. Kontrollen – og vores re-performance – viser flere fejl og mangler på de udvalgte stikprøver.

På baggrund af ovenstående vurderes det således, at fem af forvaltningerne forsat skal arbejde med registrerings- og kontrolprocedurer på området. Dette vurderes særlig væsentligt i BUF og SOF, som står for over 90 % af kommunens transaktioner på området.

Forvaltningerne har igangsat yderligere initiativer for at udbedre dette forhold, herunder har:

- BUF valgt at udskifte anvendelsen af Visa/DanKort til Eurocard, da der opleves en bedre bilagshåndtering i forvaltningen ved anvendelse af Eurocard.
- SOF, tester en app-løsning, som rulles ud i hele forvaltningen, da der opleves en bedre bilagshåndteringen ved brug af denne, ligesom der er iværksat løbende møder med de underliggende enheder for at forbedre processen og dokumentationen.

Ledelsen er bekendt med, at dette medfører en øget risiko for, at tilsigtede og utilsigtede fejl, mangler, herunder uregelmæssigheder eller besvigelser, kan opstå og forblive uopdagede.

De interne kontroller omkring bogføring og betalingsformidling er i al væsentlighed baseret på, at:

- særlige rettigheder og kritiske roller i udbetalingssystemer begrænses mest muligt, og at der ved tildeling af jobfunktions- og funktionsroller så vidt muligt, undgås konflikter med hensyn til funktionsadskillelse,
- kommunen har implementeret supplerende kontroller rettet mod medarbejdere med særlige rettigheder, kritiske roller og funktionsroller, der konflikter med hensyn til funktionsadskillelse, ændringer af betalingsoplysninger i stamdata m.v.,
- alle transaktioner gennemføres, som hovedregel, med to godkendere (4 øjnes-princip), idet betaling af eksterne fakturaer/indkøbsordre under 10.000 kr. gennemføres i henhold til kommunens forretningsgange, dog kun med én godkender, og
- der forinden betaling af leverandørfakturaer attesteres/varemodtages for, at varen er modtaget i rette mængde, kvalitet og pris.

Bogføring og betalingsformidling med kun én godkender medfører en iboende risiko for fejl i årsregnskabet, herunder fejl forårsaget af besvigelser. Risikoen relaterer sig primært til bevidste fejl, som sædvanligvis søges skjult eller sløret. Der er i tilknytning hertil etableret en kompenserende opdagende stikprøvevis kontrol af fakturaer/indkøbsordrer under 10.000 kr.

Endvidere er der helt overordnet etableret kompenserende opdagende kontroller, som mindsker risikoen for, at væsentlige fejl forbliver uopdagede. Der kan henføres til, at:

- der foretages løbende budget-/bevillingskontrol, herunder forbrugsovervågning, og
- balancekonti afstemmes løbende og er underlagt kontrol.

Vi skal gøre opmærksom på, at bemærkningerne alene har til formål at påpege de fra et revisionsmæssigt synspunkt foreliggende kontrolsvagheder. Vi skal understrege, at vi under vores revision ikke har konstateret konkrete forhold, der giver anledning til mistanke om tilsigtede eller utilsigtede uregelmæssigheder eller besvigelser som følge af ovenstående forhold.

Der henvises til afsnit 3 og 4 for uddybning af ovenstående og andre relevante forhold.

3 Observationer, risikovurderinger og anbefalinger

For nærmere beskrivelse af kategoriernes prioritet henvises til **Bilag 1 - Formidling af væsentlighed og risiko m.v.**

3.1 Nye bemærkninger og observationer 2024

Der er følgende nye kritiske eller væsentlige observationer i forbindelse med den udførte revision i 2024.

3.1.1 Observationer, der er rettet mod ØKF

Forvaltning	ØKF	**Revisionsområde**	Autorisation	**Væsentlighedsniveau**
Reference	3.1.1.1	**Revisionsemne**	Administration af autorisationer til Kvantum	
Observation	Der er foretaget analyse af SAP Basis-adgange. Baseret på SAP Basis-analyserne er der konstateret en KK-bruger samt en KMD-bruger i Kvantum, som har kritiske rettigheder til produktionsmiljøet, hvilket giver mulighed for omgåelse af kontrolmiljøet. Det er oplyst, at rollerne er givet på baggrund af et "arbejdsbetinget behov". Det er oplyst, at opgaveløsningen ikke sker gennem Firefighter- eller PIM-løsningen, der logger ændringer i produktionsmiljøer og giver mulighed for at overvåge medarbejdernes arbejde.			2024
Revisionsbemærkning	Da de kritiske rettigheder er tildelt ud fra et arbejdsbetinget behov, henstiller vi til, at der: ▶ foretages en dokumenteret risikovurdering af medarbejderens rettigheder, herunder i forhold til risikoen for besvigelser ▶ på baggrund af risikovurderingen foretages en ledelsesmæssig vurdering af, om der bør indføres kontroller til imødegåelse af de identificerede risici.			

Forvaltning	ØKF	**Revisionsområde**	Autorisation	**Væsentlighedsniveau**
Reference	3.1.1.2	**Revisionsemne**	Administration af autorisationer til Kvantum	
Observation	Den tilbagevendende analyse af funktionsadskillelseskonflikter (SoD-konflikter) i Kvantum har i 2024 afdækket, at der på tre områder er forekommet SoD-konflikter og der er i flere tilfælde potentielt sket overtrædelse af konflikterne. For to af konflikterne er det samme bruger, der har været genstand for konflikten mens der for den sidste er flere brugere. Det vedrører nedenstående tre SoD-konflikter: ▶ F005 Maintain Bank Master Data & AP Payments ▶ P003 Process Vendor Invoices & AP Payments ▶ P060 Process Vendor Invoices & Release Blocked Invoices.			2024
Revisionsbemærkning	Vi henstiller til, at arbejdet tilrettelægges således, at opgaverne kan løses uden at der forekommer SoD-konflikter.			

3.1.2 Observationer, der er rettet mod Forvaltningerne

Forvaltning	BUF og SOF	**Revisionsområde**	Bilagskontrol	**Væsentlighedsniveau**
Reference	3.1.2.1	**Revisionsemne**	Bilagskontrol	
Observation	Vi har påset, at BUF og SOF i 2024 har etableret en central stikprøvevis bilagskontrol, der skal sikre fyldestgørende og tilstrækkelig dokumentation for registreringer og udbetalinger relateret til dankort og udlæg. Bilagskontrollen viser en lang række fejl, som forvaltningerne har rettet op på. De konstaterede fejl kan væsentligst henføres til manglende oplysning omkring formål og deltagere samt mangler i forhold til tilstrækkelig dokumentation for de foretagne indkøb. BUF og SOF står for over 90 % af kommunens dankort og tilhørende transaktioner. Vores udførte re-performance af kontrollen viser et tilsvarende billede. Vi vurderer, at etableringen af den centrale bilagskontrol er en væsentlig styrkelse af kontrolmiljøet, men grundet den høje fejlrate i den stikprøvevise kontrol, må der fortsat forventes et højt antal fejl og mangler i de løbende registreringer. BUF og SOF har yderligere igangsat flere tiltag som ligeledes skal medvirke til at forbedre de regnskabsmæssige registreringer blandt andet: ▶ BUF valgt at udskifte anvendelsen af Visa/DanKort til Eurocard, da der opleves en bedre bilagshåndtering i forvaltningen ved anvendelse af Eurocard. ▶ SOF tester en app-løsning, som rulles ud i hele forvaltningen, da der opleves en bedre bilagshåndteringen ved brug af denne, ligesom der er iværksat løbende møder med de underliggende enheder for at forbedre processen og dokumentationen.			 2017 2018 2019 2020 2021 2022 2023 2024
Revisionsbemærkning	Vi vurderer, at BUF og SOF har foretaget en væsentlig styrkelse af kontrolmiljøet ved indførelse af bilagskontrollen. Bilagskontrollen – og vores re-performance – viser dog fortsat flere fejl og mangler, som forvaltningerne løbende påtaler og berigtiger. Da kontrollen er stikprøvevis, må det forventes, at der fortsat er væsentlige fejl og mangler i den samlede population i de to forvaltninger, som er udfordret af en stor volumen i forhold til anvendelse af dankort. Revisionsbemærkningen ændres derfor i 2024 fra rød til gul. Vi henstiller til, at arbejdet med at sikre fyldestgørende og tilstrækkelig dokumentation for de regnskabsmæssige registreringer i forbindelse med anvendelse af dankort og udlæg fortsætter.			

Forvaltning	ØKF, SUF og TMF	**Revisionsområde**	Bilagskontrol	**Væsentlighedsniveau**
Reference	3.1.2.2	**Revisionsemne**	Bilagskontrol	
Observation	Vi har påset, at ØKF, SUF og TMF i 2024 har etableret en central bilagskontrol, der skal sikre fyldestgørende og tilstrækkelig dokumentation for registreringer og udbetalinger relateret til dankort og udlæg. Vores udførte re-performance af kontrollen viser i lighed med forvaltningernes kontrol, at der er få fejl og mangler i bilagshåndteringen, som væsentligst kan henføres til indkøb ved anvendelse af dankort og refusion af udlæg.			 2017 2018 2019 2020 2021 2022 2023 2024
Revisionsbemærkning	Vi vurderer, at ØKF, SUF og TMF har foretaget en væsentlig styrkelse af kontrolmiljøet ved indførelse af bilagskontrollen. Revisionsbemærkningen ændres derfor i 2024 fra rød til grøn. Vi anbefaler, at arbejdet med at sikre fyldestgørende og tilstrækkelig dokumentation for de regnskabsmæssige registreringer i forbindelse med anvendelse af dankort og udlæg fortsætter indtil antallet af fejl og mangler indikerer, at den centrale kontrol enten kan nedjusteres eller afskaffes.			

3.2 Videreførte bemærkninger og observationer 2024

3.2.1 Observationer, der er rettet mod ØKF

Forvaltning	ØKF	**Revisionsområde**	Brugeradministration Kvantum	**Væsentlighedsniveau**
Reference	3.2.1.1	**Revisionsemne**	Brugeradministration Kvantum (SAP Basis)	
Observation	**Observation for 2023** Vi har foretaget analyse af SAP Basis-adgange. Baseret på SAP Basis-analyserne er der konstateret en række KMD-brugere i Kvantum, som har kritiske rettigheder til produktionsmiljøet, hvilket giver mulighed for omgåelse af kontrolmiljøet uden om PIM-løsningen. Forholdene medfører risiko for uautoriseret adgang og ændringer til systemer og data i Kvantum, det vil sige både tilsigtede og utilsigtede fejl. KS har oplyst, at man er opmærksom på forholdet, og at rollerettelser vil ske løbende og forventes afsluttet i Q1 2024. De konkrete forhold relaterer sig til: ▶ 30 KMD-brugere har adgang til at vedligeholde tabeller i produktionsmiljøet, hvoraf en enkelt KMD-bruger har eksekveret transaktionskoden, der giver adgangen inden for en 3-måneders periode. Det er oplyst, at det er aftalt med KMD, at der skal ske rettelser på deres roller, samt at det undersøges, om der er nogle af brugerne, der kan nedlægges og udelukkende tilgå Kvantum via Firefighter- eller PIM-løsningen. Rollerettelser vil ske løbende og forventes afsluttet Q1 2024. ▶ 30 KMD-brugere har adgang til at vedligeholde RFC-forbindelser i produktionsmiljøet, hvoraf tre KMD-brugere har eksekveret transaktionskoden, der giver adgang inden for en 3-måneders periode. Det er oplyst, at det er aftalt med KMD, at der skal ske rettelser på deres roller, samt at det undersøges, om der er nogle af brugerne, der kan nedlægges og udelukkende tilgå Kvantum via Firefighter- eller PIM-løsningen. Rollerettelser vil ske løbende og forventes afsluttet i Q1 2024. ▶ En enkelt KMD-bruger har adgang til at gå i debug change-mode, hvilket giver mulighed for at omgå autorisationskonceptet. Det er oplyst, at KMD-brugeren ikke har adgangen længere, da den efterfølgende er fjernet. **Opfølgning 2024** ▶ Antallet af KMD-brugere med adgang til at vedligeholde tabeller i produktionsmiljøet er reduceret fra 30 brugere i 2023 til en bruger i 2024. Brugeren har ikke eksekveret transaktionskoden i en 3-måneders periode. ▶ Antallet af KMD-brugere med adgang til at vedligeholde RFC-forbindelser i produktionsmiljøet, er reduceret fra 30 brugere i 2023 til to brugere i 2024, hvoraf den ene bruger har eksekveret transaktionskoden, der giver adgang inden for en 3-måneders periode. ▶ Der er ingen KMD-brugere, der har adgang til at gå i debug change-mode, hvilket giver mulighed for at omgå autorisationskonceptet.			2023 2024

Revisions-bemærkning	Da de kritiske rettigheder er tildelt ud fra et arbejdsbetinget behov, henstiller vi til, at der: ▶ foretages en dokumenteret risikovurdering af medarbejdernes rettigheder, herunder i forhold til risikoen for besvigelser ▶ på baggrund af risikovurderingen foretages en ledelsesmæssig vurdering af, om der bør indføres kontroller til imødegåelse af de identificerede risici.	

Forvaltning	ØKF	**Revisionsområde**	Brugeradministration Opus (Løn & Debitor)	**Væsentlighedsniveau**
Reference	3.2.1.2	**Revisionsemne**	Brugeradministration (privilegerede brugere)	
Observation	**Observation 2023** Vi har konstateret, at 18 eksterne brugere fra KMD er tildelt en kritisk autorisation (S_DEVELOP med OBJTYPE DEBUG og aktivitet 02) i produktionsmiljøet. Dette betyder, at brugerne er i stand til at omgå autorisationskonceptet i Opus, og dermed omgå kontrolmiljøet. Dette omfatter altså både OPUS Debitor og OPUS Løn. Denne adgang kan medføre øget risiko for omgåelse af kontrolmiljøet og efterfølgende besvigelser. **Opfølgning 2024** Der er ved revisionen konstateret 1 generisk bruger med denne kritiske autorisation, som anvendes af KMD. Følgende generiske brugere har adgang: ▶ DDIC (låst, men har været logget på i 2024) Revisionsbemærkningen ændres derfor i 2024 fra rød til gul.			2023 2024
Revisions-bemærkning	Vi henstiller til, at det sikres, at denne kritiske adgang som udgangspunkt begrænses helt i produktionsmiljøet, og udføres gennem Firefighter- eller PIM-løsningen.			

3.2.2 Observationer, der er rettet mod Forvaltningerne

Forvaltning	Forvaltningerne	**Revisionsområde**	Betaling til tiden	**Væsentlighedsniveau**
Reference	3.2.2.1	**Revisionsemne**	Kreditor	
Observation	**Betaling til tiden – Leverandørfakturaer** Indenrigs- og Økonomiministeren har i brev af den 4. februar 2019, til alle landets kommuner, understreget vigtigheden af, at det offentlige etablerer en god forretningsgang for betaling af regninger – "Kommuner og regioner bør derfor have stor fokus på at sikre en effektiv håndtering af regninger og løbende holde øje med, at regninger faktisk betales rettidigt". **Opfølgning 2024** Afrapportering på forfaldne fakturaer efter lukning af perioderne viser, at der i lighed med tidligere år sker stigninger af i antallet af forfaldne fakturaer i forbindelse med sommerferieperioden. Ifølge orientering til Budget- og regnskabskredsen af 8. november 2024 viser udviklingen fra 2023 til 2024, at beløbet og antallet af forfaldne fakturaer generelt, har været højere i indeværende år set i forhold til sidste år. Omfanget er lig tidligere højest omkring sommerferieperioden. Udgangen af regnskabsperiode 6 viser, at der er forfaldne fakturaer for ca. 13 mio. kr. Dette beløb er vokset til ca. 42 mio. kr. med udgangen af periode 7. Efterfølgende falder niveauet til omkring ca. 30 mio. kr. Betalingsbetingelserne i Københavns Kommune er løbende måned + 30 dage.			 2020 2021 2022 2023 2024
Revisionsbemærkning	I forbindelse med sommerferieperioden ses stadig en væsentlig stigning i forhold til ikke at betale regningerne til tiden. Det anbefales, at forvaltningerne har det nødvendige fokus på at sikre, at håndteringen af fakturaer i Kvantum sker løbende, og at der er et øget fokus på rettidig betaling til kommunens leverandører i sommerferieperioden.			

3.3 Lukkede bemærkninger og observationer i 2024

I 2024 er der lukket seks væsentlige observationer fra 2023:

- (3.1.3) Administration af autorisationer til Kvantum. Ved revisionen i 2023 blev det konstateret, at en generisk ServiceNoW-bruger havde fuld adgang til Kvantum. Denne bruger er lukket i starten af 2024.
- (3.1.4) Administration af autorisationer til Kvantum. Ved revisionen i 2023 blev der konstateret to SAP-support brugere med fuld adgang til SAP Kvantum-applikationen, som ikke var lukket ned efter brug. Vi har ikke konstateret sådanne forhold i 2024.
- (3.1.5) Regler for indkøb af varer og tjenesteydelser. De nuværende regler og retningslinjer i Personalebasen er opdateret, og der er udarbejdet et notat omkring personalerelaterede udgifter. Notat er godkendt i de forskellige forvaltninger, hvilket vil sikre det nødvendige ledelsesfokus i forhold til at kommunale midler anvendes til relevante kommunale formål.
- (3.2.1) Administration af autorisationer til Kvantum. Ved revisionen i 2023 blev der, som led i analysen af SoD-konflikter, konstateret en række brugere med SoD-konflikter relateret til vedligeholdelse af kontoplan og bogføring, samt én robot med SoD-konflikter. Vi har ikke konstateret sådanne forhold i 2024.

4 Udført arbejde

Revisionen har omfattet en gennemgang af følgende nøgleområder:

Område	Konklusion / anbefalinger
4.1 Væsentlige driftsprocesser på kreditorområdet i Kvantum	Revisionen har vist, at kontrollerne er implementeret og fungerer efter hensigten.
4.1.1 IDoc	
4.1.2 Stamdataspær	
4.1.3 Bank	
4.1.4 Bankmellemregning	
4.1.5 Kortluk	
4.1.6 Fejlkonti	
4.1.7 Nemkonto	
4.1.8 Kreditor	
4.2 Hierarki og prokuragrænser ved godkendelse af bilag	Revisionen har vist, at kontrollerne er implementeret og fungerer efter hensigten.
4.3 Oprettelse af manuelle fakturaer/udbetalinger direkte i Kvantum	Revisionen har vist, at kontrollerne er implementeret og fungerer efter hensigten.
4.4 Administration af autorisationer til Kvantum	Der henvises til afsnit 3.2 Videreførte bemærkninger og observationer 2024.
4.5 Kontrol af medarbejdere med særlige rettigheder i Kvantum	Revisionen har vist, at kontrollerne er implementeret og fungerer efter hensigten.
4.6 Den af KS udførte stikprøvekontrol	Revisionen har vist, at kontrollerne er implementeret og fungerer efter hensigten.
4.7 Bilagskontrol	Der henvises til afsnit 3.1 Nye bemærkninger og observationer 2024.

4.1 Væsentlige driftsprocesser på kreditorområdet i Kvantum

I fakturamodtagelsesprocessen er det en iboende risiko, at fejlagtige fakturaer modtages og godkendes til betaling, samt at der med svig for øje sker tilpasning til en fakturas betalingsoplysninger. Med det formål at opnå overbevisning for, at disse risici er afdækket, har vi identificeret relevante kontroller og gennemført handlinger, der afdækker, at kontrollerne er hensigtsmæssigt designet, er implementeret og har været effektive for hele perioden.

Vi har gennemgået systemkontrollen, der automatisk sender fakturaer over 10.000 kr. til 2.-godkendelse uden bemærkninger. Desuden er nedenstående kontroller gennemgået:

4.1.1 IDoc

IDoc-rettigheden giver muligheden for at fejlrette bilag, der er blevet stoppet i IDoc. Det er muligt at ændre i alle oplysninger for bilaget, herunder også betalingsoplysninger. Det er påset, at denne kritiske rettighed - i overensstemmelse med de interne processer - alene er tildelt medarbejdere i KS-SKC. Rettighederne tildelt i KS-kreditor er udelukkende "vis"-adgange og giver således ikke mulighed for at rette.

Alle ændringer foretaget til kritiske felter logges og udtages til efterfølgende manuel kontrol. Det er ved vores gennemgang af loggen og den udførte kontrol konstateret, at der i den reviderede periode ikke er foretaget ændringer til kritiske felter via IDoc.

4.1.2 Stamdataspær

Ved ændring til kritiske felter efter indlæsningen i Kvantum påføres leverandøren en spærre, hvilket medfører, at alle betalinger bliver stoppet. Frigivelse af leverandøren sker ved manuel kontrol af de nye oplysninger.

Vores test af kontrollen med manuel validering af nye oplysninger har ikke givet anledning til bemærkninger.

4.1.3 Bank

Processen er tilrettelagt, så alle transaktioner i banken automatisk udkonteres på mellemregningskonti. Dermed sikres det, at der ikke opstår afstemningsdifferencer på bankkonti. De modtagne afstemninger pr. 31. august 2024 viser, at der ikke fremstår afstemningsdifferencer. Det vurderes derfor, at processen med automatisk udkontering til mellemregningskonti er effektiv. Efter oplysninger fra kommunens banker, Danske Bank og Nordea, har kommunen pr. 31. august 2024 1.280 bankkonti i alt, der udviser en saldo på debet 1.040,6 mio. kr. (selvejende institutioner og beboerbank er ikke indeholdt).

4.1.4 Bankmellemregning

Vi har gennemgået forretningsgangene vedrørende håndtering af bankmellemregningskonti og testet, at afstemning af bankmellemregning er foretaget pr. 31. august 2024.

Kommunen har 86 bankmellemregningskonti med saldi i statusbalancen pr. 31. august 2024 med en nettosum på debet 5,2 mio. kr. i alt. Vi har modtaget en bankafstemning samt bankmellemregningsafstemning. Dokumentation for de enkelte afstemninger er hentet i Kvantum.

Der er udvalgt 3 konti til gennemgang. Gennemgangen har ikke givet anledning til bemærkninger.

4.1.5 Kortluk

Vi har i forbindelse med revisionen set på kontrollen af fratrådte medarbejdere. Opfølgning på fratrådte medarbejdere udføres løbende i KS.

Den nye proces for kontrollen af fratrådte medarbejdere med Visa/Dankort og Eurocard er blevet implementeret.

Vi har ved revisionen konstateret, at kontrol af betalingskort for fratrådte medarbejdere er blevet udført og har ikke givet anledning til yderligere.

4.1.6 Fejlkonti

I henhold til de autoriserede konteringsregler skal saldoen senest ved regnskabsaflæggelsen gå i nul. Der skal dog dagligt foretages en overvågning og løbende berigtigelse af kommunens fejlkonti for at sikre, at mængden af posteringer ikke bliver uoverskuelig. Derudover skal der løbende foretages sagsbehandling af de enkelte forhold, således at der sker berigtigelse af årsagerne, og at fejlene ikke opstår fremadrettet.

Vi har modtaget og gennemgået afstemninger af fejlkonti, herunder fejlkonto for Opus Debitor, for maj, august samt september. Gennemgangen har ikke givet anledning til bemærkninger.

4.1.7 NemKonto

Vi har testet den udarbejdede kontrol med, at alle ændringer til NemKonto-registeret (indberetning af alternativ modtager) sker på et validt grundlag. Ved at rekvirere loggen fra NemKonto-systemet over ændringer har vi påset, at der er udført kontrol med alle ændringer til betalingsmodtager.

4.1.8 Kreditor

Forvaltningerne skal løbende sikre sig, at fakturaer og indkøbsordrer håndteres i henhold til kommunens regler.

For at forvaltningerne kan efterleve sit ansvar i processen, er det afgørende, at KS følger op på og sikrer, at der ikke hænger fakturaer og ordrer i systemmodulerne til håndteringen af disse.

4.2 Hierarki og prokuragrænser ved godkendelse af bilag

Ved 2.-godkendelse af bilag over 10.000 kr. sker godkendelse i overensstemmelse med de i Kvantum indarbejdede prokuragrænser. En væsentlig risiko ved tildelingen af prokuragrænser er, at medarbejderens mulighed for at disponere på vegne af kommunen ikke harmonerer med den organisatorisk understøttede delegation af ansvar. Beløbsmæssige begrænsninger skal bidrage til en lavere risiko for fejldisponeringer – manglende regler for tildeling af prokuragrænser medfører en risiko for, at medarbejdere uden de nødvendige ledelsesmæssige beføjelser kan godkende og forpligte kommunen for betydelige beløb.

Prokuraudtræk for oktober 2024 viser, at alle forvaltninger fortsat er i tråd med den hierarkiske organisering, og prokuragrænserne følger det ledelsesmæssige ansvar.

4.3 Oprettelse af manuelle fakturaer/udbetalinger direkte i Kvantum

Ved manuel oprettelse af fakturaer/udbetalinger er der en øget risiko for, at tilsigtede og utilsigtede fejl, mangler, uregelmæssigheder eller besvigelser kan opstå og forblive uopdagede.

Vi har ved vores revision gennemgået processerne for oprettelse af manuelle fakturaer/udbetalinger direkte i økonomisystemet med henblik på at opnå en rimelig grad af overbevisning for, at disse risici er adresseret.

Det er i den forbindelse påset, at der er etableret en elektronisk forebyggende kontrol, som sikrer, at manuelt oprettede bilag, går i almindeligt godkendelsesflow med 2.-godkender. Såfremt der påføres betalingsoplysninger, eller der ændres i betalingsmetode, sker det i det samme kontrolspor, som vi har testet i afsnit 4.1.

De udførte handlinger har ikke givet anledning til bemærkninger.

4.4 Administration af autorisationer til Kvantum

Det er ledelsens ansvar at tilrettelægge niveauet for hensigtsmæssige og betryggende interne kontroller, og i overensstemmelse med kommunens kasse- og regnskabsregulativ m.v., er de interne kontroller omkring bogføringen og betalingsformidling i al væsentlighed baseret på, at:

- kritiske roller i økonomisystemet begrænses mest muligt, og at det så vidt muligt undgås, at der ved tildeling af jobfunktions- og funktionsroller fremkommer konflikter med hensyn til funktionsadskillelse,
- kommunen har implementeret supplerende kontroller rettet mod medarbejdere med udvidede rettigheder, kritiske roller, funktionsroller, der konflikter med hensyn til funktionsadskillelse, ændringer af betalingsoplysninger i stamdata m.v.

Vi har i forbindelse med revisionen foretaget en gennemgang af brugeradgange til udvalgte kritiske forretningsmæssige funktionsadskillelseskonflikter (SoD) i SAP Kvantum-applikationen inden for record to report, purchase to pay, order to cash. Derudover er der foretaget gennemgang af adgange til udvalgt kritisk SAP Basis-funktionalitet. Gennemgangen er foretaget med udgangspunkt i analyser udarbejdet med EY's autorisationsværktøj.

Det er oplyst, at KS i 2022 har foretaget en større gennemgang af autorisationskonceptet i SAP Kvantum-applikationen, hvilket også afspejles i de foretagne analyser.

Resultatet af EY's adgangsanalyser til hhv. SAP SoD og SAP Basis, herunder mere detaljerede tekniske oplysninger, er fremsendt særskilt til KS til videre bearbejdning. Derudover er der afholdt et afrapporteringsmøde, hvor analyserne blev fremlagt.

Vores bemærkninger til gennemgangen fremgår af afsnit 3 samt vores rapportering vedrørende generelle IT-kontroller.

4.5 Kontrol af medarbejdere med særlige rettigheder i Kvantum

Vi har i lighed med sidste år konstateret, at der fortsat er mulighed for at foretage enegodkendelser. Dette skyldes, at visse kombinationer af enkeltroller i praksis giver samme rettigheder, som den tidligere særlige rettighed (Kreditor kritisk).

Kombinationen af nedenstående roller giver samme mulighed som den tidligere Kreditor kritisk:

- F_FICB_FKR – aktivitet 10 (bogføre i Finans)
- M_RECH_WRK – aktivitet 77 (forudregistrere i MIR4)
- M_RECH_WRK – aktivitet 01 (bogføre i MIR4).

Der er etableret arbejdsgange, som foreskriver, at der ikke må foretages bogføringer med enegodkendelse, med undtagelse af ved den overvågede proces omkring lukning af fakturapuljen.

Hvis der fejlagtigt bliver bogført med enegodkendelse, er der designet og implementeret en kontrol af alle bilag.

Revisionen har vist, at kontrollen er implementeret og har været effektiv for året.

Ledelsen er opmærksom på, at enegodkendelse er en afvigelse til hovedreglen med funktionsadskillelse (to godkendere), som således ikke er implementeret fuldt ud i forbindelse med tildeling af rettigheder.

Det er ledelsens vurdering, at de etablerede kontroller er tilstrækkelige, og at en ændring af Kvantum ikke vil stå mål med den økonomiske udgift forbundet med ændringen.

4.6 Den af KS udførte stikprøvekontrol

Det betragtes som god governance, at ledelsen løbende sikrer sig, at der er et effektivt internt kontrolmiljø, som sikrer overholdelse af gældende regler og forskrifter, og som adresserer væsentlige risici.

I Københavns Kommune er der etableret en intern kontrol (bilagskontrol), som udføres af KS. Formålet med kontrollen er at påse, hvorvidt kommunens regnskabsføring er i overensstemmelse med formkravene i gældende regler fra ministeriet og at opnå overbevisning for registreringernes rigtighed som grundlag for regnskabet.

Det er konstateret, at KS har udført og udsendt ledelsesinformation for hele 2024. På tidspunktet for rapporteringen har vi modtaget til og med oktober måned.

Vi har foretaget en re-performance af KS's udførte kontrol med Finansposteringer, Udlæg og Dankort samt udførte kontrol af fakturaer under 10.000 kr. Hvilket ikke har givet anledning til bemærkninger.

4.7 Bilagskontrol

Med henblik på at opnå forståelse af kontrolmiljøet af udlæg og dankort, har vi foretaget test af forvaltningernes etablerede egenkontroller. Dette er foretaget gennem interview af de respektive kontrolejere samt efterprøvelse af kontrollerne.

Vi har desuden gennemgået fakturaer over 90 mio. kr. for perioden januar – august 2024 for at vurdere, hvorvidt der har været vedhæftet tilstrækkelig dokumentation til bilagene samt at procura ved godkendelse inden betaling er efterlevet.

4.7.1 Fakturaer over 90 mio. kr.

Vores gennemgang af fakturaer over 90 mio. kr. i Kvantum har vist, at der er vedhæftet den fornødne dokumentation i form af kontrakter eller lignende, og kommunens procura for 2.-godkendelse er fulgt.

4.7.2 Central kontrol af bilag

Vi har testet forvaltningernes centrale kontrol af bilag, som udføres på udvalgte bilagstyper for at bidrage til fyldestgørende og tilstrækkelig dokumentation for de regnskabsmæssige registreringer – herunder med et særligt fokus på information om formål og deltagere.

Der er forskel på, hvor langt i processen forvaltningerne er med bilagskontrollen, og vi har ved udførelsen af revisionen være i dialog med og haft forskellige anbefalinger til forvaltningerne, der primært kan henføres til en mere formaliseret metodebeskrivelse samt opfølgning på identificerede fejl og mangler.

Revisionen har dog vist, at kontrollerne generelt er implementeret og fungerer efter hensigten.

4.7.3 Visa/Dankort

Vi har ved revisionen haft fokus på kommunens anvendelse af Visa/Dankort. Vores gennemgang viser, at de fleste kort og antal transaktioner foretages i forvaltningerne BUF og SOF.

Vi har foretaget en kategoriseringen af Visa/Dankort-købene for 10 enheder ved henholdsvis BUF og SOF for perioden fra januar til maj 2024, som danner grundlag for en drøftelse med forvaltningerne omkring deres tiltag for anvendelsen.

SOF har selv foretaget en kategorisering af Visa/Dankort-køb for 2023, hvilket har vist samme indkøbsmønster. SOF har i 2024 afholdt temabaserede drøftelser med centerchefer og tilbudsledere, med fokus på forbrugs- og regeltiltag, samt planlagt opfølgende drøftelser i 2025 og frem.

BUF har på baggrund af udfordringerne med fyldestgørende og tilstrækkelig dokumentation ved brugen af Visa/Dankort, valgt at konvertere til Eurocard med udgangen af 2024.

5 Afslutning

De konstaterede forhold har været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

Yderligere spørgsmål eller kommentarer til rapporten kan rettes til EY, Ulrik B. Vassing på telefon 25 29 45 54 eller Intern Revision, Jesper Andersen på telefon 20 42 90 88.

København, den 12. december 2024
EY Godkendt Revisionspartnerselskab

Københavns Kommune

Ulrik B. Vassing
statsautoriseret revisor

Jesper Andersen
revisionschef

Rasmus F. Andersen
statsautoriseret revisor

6 Bilag - Formidling af risiko og væsentlighed m.v.

Vi har i nærværende revision vurderet graden af risiko og væsentlighed for de enkelte observationer, og i tilknytning til den givne observation er påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med 🔴
Prioritet 1-markeringer anvendes for forhold, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en revisionsbemærkning.
Et forhold anses for kritisk, såfremt der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt og/eller har en betydelig udbredelse.
Prioritet 1-markeringer rapporteres til ledelsen med påkrav om, at disse forelægges for det stående udvalg eller Økonomiudvalget.
Prioritet 2 – markeres med 🟡
Prioritet 2-markeringer anvendes for forhold, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre revisionsbemærkninger i årsberetningen.
Et forhold anses for væsentlig, såfremt der er en middel grad af sandsynlighed for, at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse.
Prioritet 2-markeringer rapporteres til ledelsen i den reviderede forvaltning.
Prioritet 3 – markeres med 🟢
Anvendes for forhold, der ikke har givet anledning til omtale eller kun anses for mindre væsentlige, og som derfor kun rapporteres til ledelsen som opmærksomhedspunkter.
En risiko anses for mindre væsentlig, såfremt der er en lille grad af sandsynlighed for, at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jesper Gjøtterup Andersen
Revisionschef
På vegne af: Københavns Kommune
Serienummer: 068d0300-58d8-4d28-8673-0565d0fb9ff8
IP: 193.169.xxx.xxx
2024-12-12 12:20:14 UTC

Rasmus Friborg Andersen
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: e219fbda-f2e4-4cf2-b051-b646c7d11872
IP: 79.142.xxx.xxx
2024-12-12 12:45:36 UTC

Ulrik Benedict Vassing
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: 732cb4e7-8215-446a-997c-ab4b20a9363c
IP: 93.165.xxx.xxx
2024-12-12 13:51:50 UTC

Københavns Kommune

Revision af generelle IT-kontroller 2024

Økonomiforvaltningen
Att.: Adm. direktør Søren Hartmann Hede
Direktør Nicolai Kragh Petersen
Københavns Rådhus
1599 København V

Intern Revision

Building a better working world

1 Formål, omfang m.v.

Som led i den løbende revision af Københavns Kommunes regnskab for 2024 har vi foretaget revision af generelle IT-kontroller, som understøtter kommunes regnskabsaflæggelse.

Rapporten skal ses i sammenhæng med revisionsrapporten "Regnskabsføring, forretningsgange og interne kontroller", hvor en række forhold relateret til brugerstyringen i Kvantum er opsummeret.

1.1 Revisionens formål

Revisionen af de generelle IT-kontroller er en del af den lovpligtige revision og indgår i grundlaget for vores påtegning af Københavns Kommunes årsregnskab. De generelle IT-kontroller skal forstås som kontroller, som ledelsen har etableret for at understøtte og sikre funktionen af forretningssystemer, IT-baserede kontroller, og underliggende IT-infrastruktur, som har betydning for Københavns Kommunes regnskabsaflæggelse. Som en del af revisionen udvælges desuden enkelte IT-områder til den lovpligtige forvaltningsrevision.

Hovedformålet med gennemgangen af de generelle IT-kontroller omkring Kvantum, KMD Opus Debitor, KMD Opus Løn, KY og KSD, er dels at understøtte valget af revisionsstrategi samt påtegningen af årsregnskabet og dels at understøtte den lovpligtige forvaltningsrevision. Gennemgangen er derfor ikke foretaget med henblik på at identificere og evaluere effektiviteten af alle generelle IT-kontroller eller potentielle forbedringer i etablerede processer og kontroller, men alene de kontroller, som har betydning for regnskabsaflæggelsen.

Det bedste værn mod uregelmæssigheder er hensigtsmæssige forretningsgange og gode interne kontroller, hvorfor vores revision i vidt omfang har baseret sig på efterprøvelse af forretningsgange og interne kontroller, men ikke undersøgelser specielt med henblik på opdagelse af uregelmæssigheder.

Det påhviler ledelsen at tilrettelægge kontrolsystemer og forretningsgange, der er betryggende efter forvaltningens forhold, og det påhviler revisor at gennemgå disse forretningsgange og interne kontroller som et led i revisionen af årsregnskabet.

1.2 Revisionens omfang og afgrænsning

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for væsentlige fejl.

Det er ledelsens ansvar at tilrettelægge niveauet for hensigtsmæssige og betryggende interne kontroller i overensstemmelse med god IT-skik og kommunens kasse- og regnskabsregulativ m.v.

Revisionen er baseret på en forventning om, at der er tilrettelagt et velfungerende internt kontrolsystem og en pålidelig bogføring. Dette indebærer, at det overordnede kontrolmiljø og de organisatoriske rammer understøtter et velfungerende ledelses- og kontrolsystem, og at der på de enkelte aktivitetsområder er beskrevet og implementeret interne kontroller, som reducerer risikoen for væsentlige fejl til et acceptabelt niveau.

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for væsentlige fejl i regnskabsaflæggelsen.

Vi skal gøre opmærksom på, at revisionen først anses for afsluttet, når vi har underskrevet erklæringen på årsregnskabet.

Lovpligtig revision:

Revisionen er tilrettelagt således, at ikke alle områder gennemgås hvert år; dog således, at alle for regnskabets væsentlige områder bliver gennemgået årligt, samt væsentlige kontrolsvagheder altid bliver fulgt op ved efterfølgende års revision. Revisionen har omfattet en vurdering af de generelle IT-kontroller inden for følgende områder for Kvantum, KMD Opus Debitor, KMD Opus Løn, KY og KSD:

Logiske adgangskontroller:

- Processer for brugeradministration, herunder oprettelse, nedlæggelse og periodisk gennemgang af brugeradgange
- Sikkerhedsindstillinger
- Krav til adgangskoder
- Privilegerede adgange, herunder funktionsadskillelse i adgangskontrollerne
- Adgange til kritisk IT-funktionalitet

Ændringshåndtering:

- Processer for vedligeholdelse af KMD Opus Debitor, KMD Opus Løn, KY og KSD, herunder at ændringer inden implementering i de produktive miljøer er;
  - Autoriseret
  - Testet
  - Godkendt
  - Samt at der er funktionsadskillelse processen.

Operations:

- Patch management
- Backup og retablering af data.

Revisionen af de generelle IT-kontroller har ikke omfattet en vurdering af kontrol- og sikkerhedsniveauet i de enkelte brugersystemer, herunder automatiske kontroller i de administrative processer og logiske adgangsrettigheder til udførsel af forretningsaktiviteter i brugersystemerne.

Københavns Kommune har aftale med KMD omkring drift af Kvantum, KMD Opus Debitor og KMD Opus Løn, samt tilhørende platforme. Yderligere har kommunen en aftale med Kombit omkring drift af applikationerne KY og KSD.

Der modtages årligt en revisionserklæring for de generelle IT-kontroller omfattende KMD's generelle driftsydelser, samt en årlig specifik erklæring for Kvantum, KMD Opus Debitor og KMD Opus Løn. For så vidt angår KY- og KSD-applikationerne modtages der også årligt specifikke erklæringer. Revisionserklæringerne forventes modtaget i Q1 2025 dækkende 2024.

Forvaltningsrevision:

Forvaltningsrevisionen har omfattet følgende områder:

- Ledelsestilsyn med brugerautorisationer (opfølgning på tidligere observationer)
- Ibrugtagning af IT-systemer (opfølgning på tidligere observationer)
- Risikovurderinger af IT-systemer (opfølgning på tidligere observationer)
- Organisering af informationssikkerhed og styrkelse af ISMS (opfølgning på tidligere observationer).

1.3 Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2024, og ved interviews af relevante personer hos Københavns Kommune samt ved observation og stikprøvevis gennemgang af udleveret materiale.

2 Ledelsesresumé og konklusion

2.1 Lovpligtige revision

Den lovpligtige revision af IT-området har blandt andet haft fokus på brugerstyringen i de IT-systemer, som vurderes kritiske for regnskabsaflæggelsen.

Vi kan konstatere, at KK generelt har et velfungerende kontrolmiljø omkring kritiske rettigheder, som tildeles midlertidigt ("PIM-løsningen").

Vi har herudover konstateret områder omkring sikkerhedsopsætning og ændringshåndtering som bør styrkes i Kvantum.

Der henvises til afsnit 3 for uddybning af ovenstående og andre relevante forhold.

2.2 Forvaltningsrevision med fokus på informationssikkerhed

Truslerne på informationssikkerhedsområdet er konstant stigende og antallet af virksomheder og myndigheder, der har været udsat for alvorlige hændelser som følge af cyberangreb eller andre alvorlige IT-sikkerhedsmæssige hændelser er tilsvarende stigende.

Siden 2021 har revisionen løbende påpeget behovet for styrkelse af informationssikkerheden i KK, herunder etablering af et passende ledelsessystem for informationssikkerhed (ISMS) baseret på ISO27001, og et tilhørende SoA-dokument.

Et velfungerende ledelsessystem, og implementering af passende sikkerhedsforanstaltninger, baseret på konkrete og aktuelle risikovurderinger, er med til at underbygge om det aktuelle informationssikkerhedsniveau er tilstrækkeligt ift. kommunens risikoappetit og kan ligeledes bidrage til at styre økonomien forbundet med at opretholde det sikkerhedsniveau, som ledelsen har besluttet. Styrer man efter ISO-27001 kan der derfor også skabes indblik i, om de økonomiske rammer anvendes bedst muligt ift., hvor der skabes mest værdi for de overordnede informationssikkerhedsmæssige beslutninger.

ØKF har igangsat et ISMS-projekt i erkendelse af, at der er behov for yderligere styrkelse og forbedringer i forhold til drift og vedligeholdelse af kommunens ledelsessystem.

Vi har noteret os, at status på dette arbejde i november 2024 er følgende:

- **Styrkelse af ledelsessystemet for informationssikkerhed baseret på ISO 27001 (ISMS)**

Kredsen af IT-direktører i KK havde den 15. november 2024 en temadrøftelse om informationssikkerhed opdelt i fire indsatsspor:

- Organisering og snitflader
- ISMS – opbygning og systemunderstøttelse
- NIS2
- Aktivitets- og udgiftsniveau.

Det endnu er uvist, hvordan kommuner bliver omfattet af NIS2-direktivet, og dermed uvist om der kommer finansiering i form at DUT-kompensation.

De fire indsatsspor er opsat i et roadmap, som giver overblik over de kommende indsatser og kendte milepæle. I materialet indgår også et kort oprids af informationssikkerhed, rolle- og ansvarsfordelingen på informationssikkerhedsområdet.

Det fremgår, at ISMS-opbygning og systemunderstøttelse forventes at løbe helt frem til Q4 2026.

- **Vurdering af, hvorledes styring af informationssikkerhed mest hensigtsmæssigt organiseres og styrkes**

I 2023 blev der under revisionsgennemgangen identificeret en væsentlig mangel på et formelt informationssikkerhedsledelsessystem (ISMS) i Københavns Kommune. Som en del af blandt andet NIS2-projektet er der planlagt en implementering af et ISMS, der skal styrke informationssikkerheden og sikre en struktureret tilgang til governance og risikostyring. Et effektivt ISMS kræver et klart dokumenthierarki, som understøtter systematisk risikohåndtering og rapportering til ledelsen.

Vores gennemgang heraf er fortsat igangværende, og vi vil foretage en særskilt afrapportering herpå.

Vi noterer, at KK har ansat en CISO, som tiltræder 1. december 2024, og der er i forbindelse hermed udmeldt en ny organisering af informationssikkerhedsområdet i KIT.

Risikovurderinger af IT-systemer

Et element i et velfungerende ISMS er effektiv planlægning baseret på risikovurderinger for alle væsentlige IT-aktiver, herunder systemer og processer.

I 2023 anførte vi, at de nuværende risikovurderinger af systemer bør styrkes, så det sikres, at alle relevante systemer bliver omfattet og med afsæt i opdaterede trusselsvurderinger, herunder at der sker en dokumenteret opfølgning på at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt.

Vi har noteret os, at KK fra den 31. oktober 2024 anvender et nyt risikovurderingskoncept i forbindelsen med nyanskaffelser af IT-systemer, og at der arbejdes på en fællesadministrativ forretningsgang, som skal klarlægge roller og ansvar i forbindelse med risikovurderinger i KK. Dette arbejde vil desuden klarlægge omfang og frekvens for risikovurdering af kommunens idriftsatte systemer.

Overordnet er det EY's vurdering, at den nye risikovurderingsmodel ikke metodisk følger alle områder i ISO 27005-standarden. Man har dog gjort sig nogle fornuftige overvejelser til processen, men samlet set vil det være vanskeligt at anvende resultaterne for risikovurderingerne i KK's overordnede IT-risikostyring.

Sikkerhedsvurdering af IT-systemer

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.

Vi har noteret os, at KK i 2024 har udført et stort arbejde med at få udarbejdet sikkerhedsvurdering af et stort antal systemer, i forlængelse af revisionens bemærkning herom fra 2023.

Vores opfølgning i 2024 viser, at man ikke er helt i mål med arbejdet i forhold til at sikre, at kommunens regler er efterlevet fuldt ud.

Ledelsestilsyn med brugerautorisationer

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.

En stikprøvevis gennemgang i 2023 viste, at de ledelsestilsyn ikke fuldt ud udføres i overensstemmelse med kommunens regler. Det gælder både de systemer, der er integreret i IGA-løsningen og med overvejende sandsynlighed også de systemer, der ligger uden for IGA-løsningen.

Ved at integrere et system i kommunens IGA-løsning vil hyppigheden for ledelsestilsyn kunne minimeres betragteligt, hvis de rette foranstaltninger etableres.

Vi har noteret os, at forvaltningerne i 2024 har igangsat et stort arbejde med korrekt mærkning af data i FISKK, få integreret flere systemer i kommunens IGA-løsning og få udført de krævede ledelsestilsyn, i forlængelse af revisionens bemærkning herom fra 2023.

Vores opfølgning i 2024 viser, at man ikke er helt i mål med arbejdet i forhold til at sikre, at kommunens regler er efterlevet fuldt ud.

Der henvises til afsnit 3 for uddybning af ovenstående og andre relevante forhold.

3 Observationer, risikovurdering og anbefaling

For nærmere beskrivelse af kategoriernes prioritet henvises til
Bilag 1 - Formidling af væsentlighed og risiko m.v.

3.1 Nye kritiske bemærkninger og væsentlige observationer i forbindelse med den udførte IT-revision

Forvaltning	ØKF	**Revisionsområde**	ISMS	**Væsentlighedsniveau**
Reference	3.1.1	**Revisionsemne**	Organisering af informationssikkerhed og styrkelse af ISMS	
Observation	*Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System).* I 2016 indgik KL, sammen med en række andre offentlige myndigheder, en aftale, der forpligtede kommunerne at følge principperne i informationssikkerhedstandarden ISO-27001. ISO-27001 er en international standard for informationssikkerhedsstyring, som giver en systematisk og risikobaseret tilgang til informationssikkerhed. Ifølge ISO-27001 er informationssikkerhed et ledelsesansvar. ISO-27001 opererer med et ledelsessystem for informationssikkerhed – ofte benævnt 'ISMS' (Information Security Management System) – som indeholder alle de politikker, procedurer, retningslinjer og tilhørende ressourcer og aktiviteter m.m., som en organisation administrerer for at beskytte sine informationsaktiver. Et velfungerende ledelsessystem, og implementering af passende sikkerhedsforanstaltninger, baseret på konkrete og aktuelle risikovurderinger, er med til at underbygge om det aktuelle informationssikkerhedsniveau er tilstrækkeligt ift. kommunens risikoappetit, og kan ligeledes bidrage til at styre økonomien forbundet med at opretholde det sikkerhedsniveau, som ledelsen har besluttet. Styrer man efter ISO-27001 kan der derfor også skabes indblik i, om de økonomiske rammer anvendes bedst muligt ift., hvor der skabes mest værdi for de overordnede informationssikkerhedsmæssige beslutninger.			2023 2024
Revisionsbemærkning	ØKF oplyser, at ISMS-opbygning og systemunderstøttelse forventes at løbe fra Q4 2024 frem til Q4 2026. Det er vores vurdering, at den konstant stigende trussel på informationssikkerhedsområdet, skærpet lovgivning på området samlet set øger risikoen yderligere i forhold til informationssikkerheden i KK. Revisionsbemærkningen ændres derfor i 2024 fra gul til rød. Vi henstiller, at forvaltningerne styrker indsatsen omkring organisering af informationssikkerheden og etablering af et ISMS (Information Security Management System) i de fire indsatsspor, som er besluttet i kredsen af IT-direktører: ▶ Organisering og snitflader ▶ ISMS – opbygning og systemunderstøttelse ▶ NIS2 (hvis KK bliver omfattet) ▶ Aktivitets- og udgiftsniveau.			

	I forbindelse hermed anbefales, at der er stort ledelsesmæssigt fokus på at sikre den nødvendige fremdrift og de nødvendige ressourcer og kompetencer i programmet.	

Forvaltning	ØKF	**Revisionsområde**	Risikovurderinger	**Væsentlighedsniveau**
Reference	3.1.2	**Revisionsemne**	Risikovurderinger af it-systemer	
Observation	*Risikovurderinger af IT-systemer* 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 konsekvent foretages en dokumenteret vurdering af, hvorvidt de mitigerende sikringstiltag og kontroller faktisk fungerer hensigtsmæssigt. **Status 2024** ØKF har besluttet og igangsat en handleplan, hvorefter KK fra den 31. oktober 2024 anvender et nyt risikovurderingskoncept i forbindelsen med nyanskaffelser af IT-systemer. Der arbejdes på en fællesadministrativ forretningsgang, som skal klarlægge roller og ansvar i forbindelse med risikovurderinger i KK. Dette arbejde vil desuden klarlægge omfang og frekvens for risikovurdering af kommunens idriftsatte systemer. Handleplanen forventes afsluttet i Q2 2025. *Nyt risikovurderingskoncept* Overordnet er det EY's vurdering, at den nye risikovurderingsmodel ikke metodisk følger alle områder i ISO 27005-standarden og gennemgangen af skabelonen med tilhørende dokumentation indikerer ikke, at KK arbejder systematisk med IT-risikostyring. Man har dog gjort sig nogle fornuftige overvejelser til processen for udarbejdelse af risikovurderinger, men samlet set vil det være vanskeligt at anvende resultaterne for risikovurderingerne i KK's overordnede IT-risikostyring. Der ses en forskel mellem best practice, kravene i ISO27005 og KK's nye risikovurderingskoncept. Koncern IT har modtaget et notat med baggrunden i ovenstående og konkrete anbefalinger i forhold til: ► Risikobehandling ► Konsekvensområdet - tilgængeligheden i tid ► Konsekvensvurdering			2024 2023 2022

	▶ Sandsynlighedsvurdering ▶ Trusselskataloget.	
Revisionsbemærkning	Revisionsbemærkningen ændres i 2024 fra gul til rød og det henstilles at: ▶ 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.	

Forvaltning	ØKF	**Revisionsområde**	Ændringshåndtering	**Væsentlighedsniveau**
Reference	3.1.3	**Revisionsemne**	Åbning af det produktive miljø (Kvantum)	
Observation	Vi har observeret, at det produktive miljø for klient 000 er åben for programændringer. Hvis der foretages programændringer direkte i det produktive miljø i klient 000, vil det også påvirke det produktive miljø i klient 950 (Kvantum). Vi er blevet informeret om, at klienten vedligeholdes af KMD.			🔴 2024
Revisionsbemærkning	Vi henstiller til, at den nuværende åbning lukkes, og at klienten kun åbnes efter et arbejdsbetinget behov.			

Forvaltning	ØKF	**Revisionsområde**	Ændringshåndtering	**Væsentlighedsniveau**
Reference	3.1.4	**Revisionsemne**	Log af åbninger (Kvantum)	
Observation	Vi har observeret, at der er blevet foretaget to direkte tilpasninger (customizing ændringer) i systemet i det produktive miljø (klient 950). Disse ændringer er ikke blevet logget, hvilket betyder, at der ikke findes nogen registrering af, hvad der er foretaget af ændringerne. Denne mangel på logning kan føre til manglende sporbarhed af ændringer foretaget direkte i det produktive miljø.			🔴 2024
Revisionsbemærkning	Vi henstiller til, at der anvendes "recording"-funktionen, når den produktive klient åbnes for direkte customizing, hvorved der logges for eventuelle ændringer i det produktive miljø.			

Forvaltning	ØKF	Revisionsområde	Brugeradministration	Væsentlighedsniveau
Reference	3.1.5	Revisionsemne	Password opsætning (Kvantum)	
Observation	Vi har konstateret følgende svagheder omkring password profilparametre i Kvantum: ► "login/min_password_lng": Minimumslængde på password, er sat til 8 karakterer ► " login/min_password_specials": Minimum specialle tegn, er sat til 0 Manglende kompleksitet 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. Hvis adgangskoden er kort eller består af almindelige ord eller simple mønstre, kan en hacker hurtigt finde den rigtige adgangskode ved hjælp af automatiserede værktøjer.			 2024
Revisionsbemærkning	Det anbefales, at passwordopsætningen følger Københavns Kommunes passwordpolitik, som pr. 21. november 2024 stiller krav om en passwordlængde på minimum 15 karakterer, efter beslutning den 21. maj af IT-kredsen. Adgangskoderne bør bestå af en kombination af store bogstaver, små bogstaver, tal eller symboler. Vi er opmærksomme på, at der er implementeret Single Sign-On (SNC) på Kvantum, hvilket betyder, at brugerne kan logge ind på systemet én gang via Windows AD og derefter få adgang til Kvantum uden at skulle logge ind igen. Dog vil vi anbefale, at I styrker adgangskodeparametrene, da der er en risiko for, at brugere kan tilgå SAP GUI direkte. 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.			

Forvaltning	ØKF	Revisionsområde	Brugeradministration	Væsentlighedsniveau
Reference	3.1.6	Revisionsemne	Gennemgang af rettigheder (Kvantum)	
Observation	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 baserer 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 fuldstændig og nøjagtig.			 2024
Revisionsbemærkning	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 er en forhøjet risiko for fejl i integrationen ved manuelle tildelinger direkte i Kvantum.			

3.2 Bemærkninger og observationer fra tidligere år, og hvortil det vurderes, at disse videreføres i indeværende år

Forvaltning	Forvaltningerne	**Revisionsområde**	Brugerautorisationer/IGA/IAM	**Væsentlighedsniveau**
Reference	3.2.1	**Revisionsemne**	Ledelsestilsyn med bruger autorisationer	
Observation	*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	 2024 2023	

	4. Genbesøg af informationssikkerhedscirkulæret 5. Fortsættelse af igangværende udviklingsopgaver mhp. Effektiv administration. Handleplanen forventes gennemført i perioden Q4 2024 til ultimo 2025.	
Revisions-bemærkning	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-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.	

Forvaltning	Forvaltningerne	Revisionsområde	Ibrugtagningstilladelser på IT-systemer	Væsentlighedsniveau
Reference	3.2.2	Revisionsemne	Sikkerhedsvurdering af systemer	
Observation	*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. 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. 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. **Status 2024** Forvaltningernes har besluttet og 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 nødvendigheden af eskalation, ny sikkerhedsvurdering eller udfasning af ikke-godkendte IT-systemer. Handleplanen forventes gennemført i perioden Q4 2024 til Q2 2025.			2024 2023 2022
Revisionsbemærkning	Bemærkningen videreføres og i lighed med tidligere år henstilles det, at ▶ 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, blandt andet om udfasning, idet disse, jf. kommunes regler, udgør en sikkerhedsrisiko.			

3.3 Bemærkninger og observationer fra sidste år, der i forbindelse med IT-revisionen er konstateret lukket

I 2024 er der ikke lukket observationer fra 2023.

4 Afslutning

De konstaterede forhold har været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

Yderligere spørgsmål eller kommentarer til rapporten kan rettes til EY, Ulrik B. Vassing på telefon 25 29 45 54 eller Intern Revision, Jesper Andersen på telefon 20 42 90 88.

København, den 12. december 2024
EY Godkendt Revisionspartnerselskab

Københavns Kommune

Ulrik B. Vassing
statsautoriseret revisor

Jesper Andersen
revisionschef

Rasmus F. Andersen
statsautoriseret revisor

5 Bilag - Formidling af risiko og væsentlighed m.v.

Vi har i nærværende revision vurderet graden af risiko og væsentlighed for de enkelte observationer, og i tilknytning til den givne observation er påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med 🔴
Prioritet 1-markeringer anvendes for forhold, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en revisionsbemærkning.
Et forhold anses for kritisk, såfremt der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt og/eller har en betydelig udbredelse.
Prioritet 1-markeringer rapporteres til ledelsen med påkrav om, at disse forelægges for det stående udvalg eller Økonomiudvalget.
Prioritet 2 – markeres med 🟡
Prioritet 2-markeringer anvendes for forhold, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre revisionsbemærkninger i årsberetningen.
Et forhold anses for væsentlig, såfremt der er en middel grad af sandsynlighed for, at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse.
Prioritet 2-markeringer rapporteres til ledelsen i den reviderede forvaltning.
Prioritet 3 – markeres med 🟢
Anvendes for forhold, der ikke har givet anledning til omtale eller kun anses for mindre væsentlige, og som derfor kun rapporteres til ledelsen som opmærksomhedspunkter.
En risiko anses for mindre væsentlig, såfremt der er en lille grad af sandsynlighed for, at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jesper Gjøtterup Andersen
Revisionschef
På vegne af: Københavns Kommune
Serienummer: 068d0300-58d8-4d28-8673-0565d0fb9ff8
IP: 193.169.xxx.xxx
2024-12-12 12:20:14 UTC

Rasmus Friborg Andersen
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: e219fbda-f2e4-4cf2-b051-b646c7d11872
IP: 79.142.xxx.xxx
2024-12-12 12:45:36 UTC

Ulrik Benedict Vassing
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: 732cb4e7-8215-446a-997c-ab4b20a9363c
IP: 93.165.xxx.xxx
2024-12-12 13:51:50 UTC

Københavns Kommune

Revisionsrapport – Revision af løn- og personaleområdet 2024

Økonomiforvaltningen
Att.: Adm. direktør Søren Hartmann Hede
Direktør Nicolai Kragh Petersen
Københavns Rådhus
1599 København V

Intern Revision

KØBENHAVNS KOMMUNE

EY
Building a better working world

1 Indledning

Som led i den løbende revision af Københavns Kommunes regnskab for 2024 har vi foretaget revision af løn- og personaleområdet.

Rapporten skal ses i sammenhæng med revisionsrapporterne "Revision af generelle IT-kontroller 2024" og "Regnskabsføring, forretningsgange og interne kontroller", hvor forhold relateret til de generelle IT-kontroller, herunder OPUS, er opsummeret.

1.1 Revisionens formål

Revision af løn- og personaleområdet er en del af den lovpligtige revision og indgår i grundlaget for revisionspåtegningen af Københavns Kommunes årsregnskab. Revisionens formål er at undersøge, om området administreres betryggende og i overensstemmelse med borgerrepræsentationens beslutninger, gældende love og andre forskrifter samt med indgåede aftaler og sædvanlig praksis. Revisionens formål er endvidere at foretage en kritisk gennemgang af de forretningsgange og kontroller, der er etableret på området.

Det bedste værn mod uregelmæssigheder er hensigtsmæssige forretningsgange og gode interne kontroller, hvorfor vores revision i vidt omfang har baseret sig på efterprøvelse af forretningsgange og interne kontroller, og ikke undersøgelser specielt med henblik på opdagelse af uregelmæssigheder.

Det påhviler ledelsen at tilrettelægge kontrolsystemer og forretningsgange, der er betryggende efter forvaltningens forhold, og det påhviler revisor at gennemgå disse forretningsgange og interne kontroller som et led i revisionen af årsregnskabet.

1.2 Revisionens omfang og afgrænsning

Omfanget af vores arbejde fastlægges ud fra vores samlede vurdering af væsentlighed og risiko for væsentlige fejl.

Det er ledelsens ansvar at tilrettelægge niveauet for hensigtsmæssige og betryggende interne kontroller i overensstemmelse med kommunens kasse- og regnskabsregulativ m.v.

Revisionen er baseret på en forventning om, at der er tilrettelagt et velfungerende internt kontrolsystem og en pålidelig bogføring. Dette indebærer, at det overordnede kontrolmiljø og de organisatoriske rammer understøtter et velfungerende ledelses- og kontrolsystem, og at der på de enkelte aktivitetsområder er beskrevet og implementeret interne kontroller, som reducerer risikoen for væsentlige fejl til et acceptabelt niveau.

Ud fra ovenstående har vi tilrettelagt vores løbende revision af løn- og personaleområdet for 2024. I forbindelse med revisionen tester vi de interne kontroller i det omfang, vi finder det nødvendigt for revisionen af årsregnskabet. Revisionen omfatter ikke en gennemgang af samtlige lønudbetalinger, men udføres ved, at vi ved stikprøver indhenter dokumentation for eller på anden måde får bekræftet udbetalingens rigtighed.

Ved gennemgangen af lønsager kategoriseres fejl og mangler i to kategorier:

- **Enkeltstående fejl og mangler**. Dette relaterer sig til forhold, hvor der ikke ligger en fejlkilde til grund, som gør, at fejlen forventes gentaget på andre sager. Dette kan sædvanligvis være taste-, tælle- eller sjuskefejl.
- **Betydelige og/eller systematiske fejl**. Dette relaterer sig til forhold, hvor det må forventes, at fejlen vil opstå i tilsvarende sager fremover, medmindre der sker en ændring. Systematiske fejl skyldes en fejl i "systemet" og må derfor forventes at opstå i tilsvarende sager, medmindre der ændres i fx forretningsgange, programmerede kontroller m.v. Betydelige fejl må forventes at opstå i tilsvarende sager af andre grunde, fx fordi lønkontorets personale har misforstået en arbejdsgang, regel m.v.

I Københavns Kommunes regnskab registreres desuden lønudgifter vedrørende en række selvejende institutioner, der har driftsoverenskomst med kommunen. Disse poster indgår tillige i særskilte regnskaber, der revideres af revisorer, som er valgt af bestyrelserne for de pågældende institutioner.

Vi skal gøre opmærksom på, at revisionen først anses for afsluttet, når vi har underskrevet erklæringen på årsregnskabet.

1.3 Revisionsarbejdets udførelse

Revisionen omfatter Intern Revisions bistand til EY i forbindelse med lovpligtig revision af løn- og personaleområdet. Revisionen er udført på grundlag af godkendt revisionsplan for 2024 og er bl.a. gennemført ved besøg hos Koncernservice (KS).

Ved revisionen har vi vurderet de processer, der er væsentlige for revisionen af kommunens årsrapport.

Revisionen har omfattet vurdering af kontrollernes:

- **Design** – og hvorvidt der på de konkrete aktiviteter er identificeret risici, som kan medføre tilsigtede eller utilsigtede fejl og mangler, og om der er udarbejdet hensigtsmæssige og betryggende forretningsgange og interne kontroller, der afdækker disse.
- **Implementering** – og om de udarbejdede retningslinjer og interne kontroller rent faktisk er implementeret i kommunen.
- **Effektivitet** – og hvorvidt kontrollen har fungeret efter hensigten og har medvirket til at forebygge eller opdage tilsigtede og utilsigtede fejl og mangler på de konkrete aktiviteter i hele regnskabsåret. Dette omfatter alene kontroller, som vurderes særlig afgørende for at sikre mod væsentlige fejl i forbindelse med kommunens regnskabsaflæggelse.

Gennemgangen har endvidere omfattet en stikprøvemæssig gennemgang af et tilfældigt udvalgt antal lønsager.

2 Ledelsesresumé og konklusion

I forbindelse med den løbende revision af lønområdet for 2024 har vi identificeret de processer, der er væsentlige for revisionen, og vurderet design og implementering af forretningsgange og interne kontroller. Hvor det bidrager til vores revisionsoverbevisning samt forståelse af kontrolmiljøet på området, har vi testet kontrollernes design, implementering og effektivitet.

Det er vores vurdering, at der generelt er etableret et kontrolmiljø, hvor automatiske og forebyggende kontroller sikrer, at fejl og mangler i al væsentlighed identificeres, og konstaterede fejl i høj grad rettes, inden vederlags- og lønudbetalingen sker.

Vores stikprøvevise gennemgang af medlemmer af Borgerrepræsentationen har ikke givet anledning til kommentarer. For øvrige lønudbetalinger har vi testet 98 lønsager, og konstateret fejl i seks af de udvalgte sager. De konstaterede fejl vurderes primært som enkeltstående fejl, hvoraf tre sager er med umiddelbar udbetalingsmæssig betydning, som kan henføres til selvejende institutioner.

Vi har konstateret, at der er fejl i grundlaget for afregningen til feriefonden af ikke-udbetalte feriepenge. Det henstilles, at omfanget afdækkes og berigtiges.

Der henvises til afsnit 3. og 4. for uddybning af ovenstående og andre relevante forhold.

3 Observationer, risikovurderinger og anbefalinger

Observationer opdeles i henholdsvis:

3.1 Nye kritiske bemærkninger og væsentlige observationer i forbindelse med den udførte revision

3.2 Videreførte bemærkninger og observationer, hvortil det vurderes, at disse videreføres i 2024.

3.3 Lukkede bemærkninger og observationer i 2024.

For nærmere beskrivelse af kategoriernes prioritet henvises til **Bilag 1 - Formidling af væsentlighed og risiko m.v.**

3.1 Nye bemærkninger og observationer 2024

Forvaltning	Forvaltningerne	**Revisionsområde**	Løn- og personaleområdet	**Væsentlighedsniveau**
Reference	4.4	**Revisionsemne**	Afregning til Feriefonden	
Observation	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. 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. 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.			 2024
Revisionsbemærkning	KS har tilrettelagt og implementeret flere fornuftige tiltag, der skal medvirke til at sikre en korrekt håndtering af ferie i forvaltningerne. 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. Desuden henstiller vi til, at KS så vidt muligt berigtiger de konstaterede fejl, der kan henføres til KS.			

Forvaltning	ØKF	Revisionsområde	Løn- og personaleområdet	Væsentlighedsniveau
Reference	4.1	Revisionsemne	Arbejdsskade	
Observation	Vores gennemgang af processen for udbetaling af arbejdsskadeerstatninger har vist, at den månedlige kontrol af stopdatoer ikke er udført for perioden januar til og med august 2024, som anført i forretningsgangen. Herudover er det konstateret, at kontrollen ikke er formaliseret/nedskrevet og ikke tilstrækkeligt dokumenteret.			2024
Revisionsbemærkning	Det henstilles, at ledelsestilsynet med at kontrollerne udføres månedligt, som anført i forretningsgangen, skærpes.			

Forvaltning	ØKF	Revisionsområde	Løn- og personaleområdet	Væsentlighedsniveau
Reference	4.3	Revisionsemne	Sagsgennemgang	
Observation	Vi har i 2024 foretaget en gennemgang af en stikprøve på 98 sager. Gennemgangen har vist fejl og mangler i seks tilfælde, som alle vurderes at være enkeltstående fejl og mangler: ▶ En fejl uden udbetalingsmæssig betydning kan henføres til manglende overholdelse af syv dags-fristen for fremsendelse af ansættelsesbrev til medarbejder. ▶ En fejl uden udbetalingsmæssig betydning kan henføres til fejl i KS ved manglende indhentelse af godkendelse for lønsammensætning fra indberetter. Sagen er berigtiget i nov. 2024. ▶ En fejl uden udbetalingsmæssig betydning kan henføres til forkert pensionskasse. I forbindelse med rettelse til korrekt pensionskasse medio juni 2024 er der ikke foretaget rettelse af allerede indbetalt pension til forkert pensionskasse for perioden 1. januar til 15. juni 2024. Sagen er berigtiget i nov. 2024. ▶ En fejl med udbetalingsmæssig betydning kan henføres til fejlagtig udbetaling af "Feriekoloni/lejrskoletillæg" i forbindelse med fratrædelse af institutionsleder. Tillægget er indberettet af enheden, som er en selvejende institution. ▶ To fejl med udbetalingsmæssig betydning vedr. forkert indtastning af timer fra vagtplansskema til KAS i en selvejende institution.			2024
Revisionsbemærkning	Der er primært konstateret enkeltstående fejl, hvoraf tre kan henføres til fejl i KS uden udbetalingsmæssig betydning, og tre sager skyldes fejl i selvejende institutioner med udbetalingsmæssig betydning. KS er enig i de observerede fejl, og vi vil senest i forbindelse med revisionen af årsregnskabet påse, at sagerne er berigtigede.			

3.2 Videreførte bemærkninger og observationer i 2024

Der er ingen videreførte bemærkninger og observationer fra 2023.

3.3 Lukkede bemærkninger og observationer i 2024

Der har ved gennemgangen i 2024 været observationer, der er lukket i 2024:

Forvaltning	ØKF	**Revisionsområde**	Løn- og personaleområdet	**Væsentlighedsniveau**
Reference	4.2	**Revisionsemne**	VIP-kontrol	
Observation	Vi konstaterede i den udførte VIP-kontrol, at der var en anmærkning i kontrollen om, at der ikke var foretaget beskatning af fri telefon under orlov uden løn. Efter reglerne fra SKAT, vil adgang til mobiltelefon, som fri telefon, medføre beskatning, også under orlov uden løn. KS er enig og har gennemgået alle BR-medlemmer med fri telefon, som har været på orlov uden løn – hvilket har medført en berigtigelse af beskatning i tre tilfælde. Desuden har BR-sekretariatet ændret i håndteringen af mobiltelefoner for BR-medlemmer og sikrer fremover en tydelig registrering samt indberetning til KS.			2024

4 Udført arbejde

Revisionen har omfattet en gennemgang af følgende nøgleområder:

Område	Konklusion / anbefalinger
4.1 Fælles obligatoriske forretningsgange (walk-through)	Gennemgangen har vist, at forretningsgangene lønkørsel og ansøgt afsked udføres i praksis som beskrevet. Der henvises til afsnit 3.1 Nye bemærkninger og observationer 2024 vedr. arbejdsskade.
Lønkørsel (Proces: Løn 1.5)	
Arbejdsskade (Proces: Løn 2.5)	
Ansøgt afsked (Proces: Løn 5.1)	
4.2 Nøglekontroller	Revisionen har vist, at kontrollerne er designet og implementeret efter hensigten. Der henvises til afsnit 3.3. Lukkede bemærkninger og observationer 2024 vedr. VIP-kontrollen.
Anormalitetskontrol	
1.- dagskontrol	
Faglig lønkontrol før og efter lønkørsel	
Faglig lønkontrol – VIP	
Særlig lønkontrol	
Lønafstemning mellem eIndkomst, lønsystem og Kvantum	
4.3 Substansrevision (sagsgennemgang)	Der henvises til afsnit 3.1 Nye bemærkninger og observationer 2024.
Stikprøvevis gennemgang af 11 vederlagssager og 98 lønsager, herunder følgende: Tilgange, Sankt Annæ Gymnasium, selvejende plejecentre med driftsoverenskomst og outliers	
4.4 Gennemgang i øvrigt	Der henvises til afsnit 3.1 Nye bemærkninger og observationer 2024.
Afregning Feriefond – afregning af ikke-afholdt eller overført ferie	

4.1 Fælles obligatoriske forretningsgange (walk-through)

Vi har vurderet design og implementering af udvalgte forretningsgange, som vurderes som værende væsentlige for lønprocessen. Dette er sket ved walk-through (vugge til grav-gennemgang) af de udvalgte forretningsgange, hvor der er foretaget en vurdering af, om forretningsgangene er designet hensigtsmæssigt. Derudover har vi efterprøvet, om processerne er implementeret som beskrevet.

Lønadministrationen foretages i 3 driftskontorer i Koncernservice, og alle driftskontorer er repræsenteret i vores walk-through. Vi har gennem walk-through opnået forståelse ved at observere sagsbehandlingen af tilfældigt udvalgte stikprøver samt interview af og forespørgsel til sagsbehandleren.

Ved gennemgangen har vi haft fokus på følgende processer:

- Lønkørsel (Proces: Løn 1.5)
- Arbejdsskade – Skattepligtig udbetaling af arbejdsskadeerstatning (Proces: Løn 2.5)
- Fratrædelse - Ansøgt afsked (Proces: Løn 5.1)

Gennemgangen har vist, at forretningsgangene vedrørende lønkørsel og fratrædelse i praksis udføres som beskrevet.

Arbejdsskade

Vores gennemgang af processen for udbetaling af arbejdsskadeerstatninger har vist, at den månedlige kontrol af stopdatoer ikke er udført for perioden januar til og med august 2024, som anført i forretningsgangen.

Herudover er det konstateret, at kontrollen ikke er formaliseret/nedskrevet og ikke tilstrækkeligt dokumenteret.

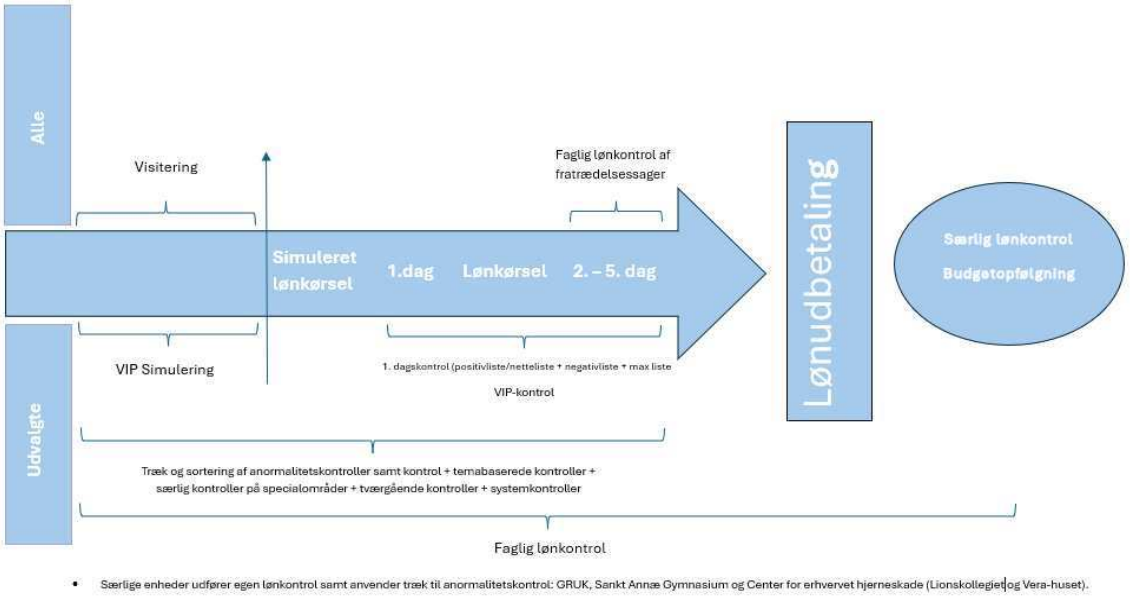
Endelig skal det nævnes, at opgaverne i håndteringen af arbejdsskade og udførelsen af kontroller er flyttet fra KEID til CLP i KS. Forretningsgangen bør ajourføres i overensstemmelse hermed.

Der henvises til afsnit 3.1 Nye bemærkninger og observationer 2024 omkring Arbejdsskade.

4.2 Nøglekontroller

Med henblik på at opnå forståelse af kontrolmiljøet på løn- og personaleområdet har vi foretaget test af nøglekontroller. Dette er foretaget gennem interviews af de respektive kontrolejere samt efterprøvelse af kontrollen.

Figur 1 - Kontrolmiljø ved månedsløn



Kilde: Egen tilvirkning

Anormalitetskontrol

Vi har testet anormalitetskontrollen, som består af udtræk og sagsbehandling af en række anormalitetsrapporter. Kontrollen bidrager til det samlede kontrolmiljø på lønområdet.

Revisionen har vist, at kontrollen er implementeret og fungerer efter hensigten.

1.-dagskontrol

Vi har revideret 1.-dagskontrollen, som omfatter udtræk og kontrol af følgende rapporter:

- Nettolisten/positivlisten
- Maxlisten
- Negativlisten
- Kontantlisten

Revisionen har vist, at kontrollen er implementeret og fungerer efter hensigten.

Faglig lønkontrol før og efter lønkørsel

Vi har testet den faglige lønkontrol – før lønkørsel på baggrund af fx en simuleret lønspecifikation og efter lønkørsel på baggrund af fx en lønkørt lønspecifikation, som udføres på udvalgte typer af lønsager. Kontrollen bidrager til det samlede kontrolmiljø på lønområdet.

Revisionen har vist, at kontrollen er implementeret og fungerer efter hensigten.

Faglig lønkontrol - VIP

Vi har testet VIP-kontrollen, som udføres på alle lønudbetalinger for borgmestre og direktører inden lønudbetaling. VIP-kontrollen skal afdække risikoen for fejl i ansættelser med særlig interesse.

Revisionen har vist, at kontrollen er implementeret og fungerer efter hensigten. Dog har gennemgangen vist, at tre BR-medlemmer ikke er blevet beskattet af fri telefon under orlov uden vederlag i henhold til SKAT's regler.

Vi henviser til afsnit 3.3 Lukkede bemærkninger og observationer 2024 omkring beskatning af fri telefon under orlov.

Særlig lønkontrol

Vi har testet den særlige lønkontrol, som udføres på alle lønudbetalinger for medarbejdere med adgange til at ændre i lønstamdata og/eller udbetale i lønsystemet eller for-systemer, der kan generere en lønudbetaling.

Revisionen har vist, at kontrollen er implementeret og fungerer efter hensigten.

Lønafstemning

Vi har påset, at KS løbende foretager lønafstemning, der sikrer, at lønudbetalinger i lønsystemet er korrekt overført til Kvantum samt korrekt indberettet til Skattestyrelsen (eIndkomst).

Vores gennemgang har ikke omfattet test af lønafstemningen ved den løbende revision. Test bliver foretaget ved den afsluttende revision af årsregnskabet 2024.

4.3 Substansrevision (sagsgennemgang)

Vi har foretaget stikprøvevis lønrevision for 2024. Lønrevisionen har til formål at sikre, at procedurerne omkring indberetning og udbetaling af vederlag, diæter og løn fungerer betryggende.

Vores revision tager afsæt i ovenstående vurdering af de arbejdsgange og interne kontroller, som har væsentlig betydning for vederlags- og løndannelsen - både centralt og decentralt. På baggrund af denne vurdering har vi udvalgt et antal vederlags- og lønsager til test af forretningsgangene.

Stikprøverne har omfattet;

- Ansatte medarbejdere i forvaltningerne
- Vederlag til politikere ved Borgerrepræsentationen, herunder overborgmesteren
- En risikorettet test af lønudbetalinger baseret på en analyse med henblik på, at identificere eventuelle indikationer på uregelmæssigheder, fejl eller afvigelser, som kan undersøges som led i revisionen.

Dette kan fx omfatte:

- Usædvanlige mønstre eller udsving i lønudbetalingerne på personniveau
- Outliers i den gennemsnitlige lønudbetaling sammenholdt med andre på samme overenskomst
- Sammenholdelse af ansættelses- og fratrædelsesdatoer ift. lønudbetalingstidspunkt

Vi har foretaget test af 11 vederlagssager og samlet set 98 personsager. Gennemgangen af diæter og vederlag har ikke givet anledning til kommentarer, mens gennemgangen af lønsager har vist fejl og mangler i seks tilfælde, som alle vurderes at være enkeltstående.

4.4 Afregning Feriefond

Vi har ved revisionen konstateret fejl i grundlaget for afregningen af ikke-udbetalte feriepenge til Feriefonden for optjeningsåret 2021/22, hvor forvaltningerne skal sikre, at indberetningerne af ferieafholdelse eller overførsel af ferie for medarbejderne håndteres korrekt.

Efter revisionens gennemgang af optjeningsåret 2021/22 har kommunen også foretaget afregning til Feriefonden af optjeningsåret 2022/23, som udgør 4,5 mio. kr., hvilket ikke er gennemgået.

Der er for optjeningsåret 2021/22 afregnet 6 mio. kr. til Feriefonden.

I samarbejde med KS, har vi gennemgået 10 sager, der har den højeste registrering af ikke-udbetalt ferie. Gennemgangen har vist fejl og mangler i alle tilfælde, der kan henføres til nedenstående;

Figur 2 – Topliste over afregning til Feriefonden i 2023 for optjeningsåret 2021/22

Medarb.	Forvaltning	Bruttoferie DKK	Antal timer	Kommentar
1	SOF	44.504,78	133,20	Barselsskema ikke håndteret korrekt - KS
2	ØKF	42.857,25	118,40	Feriehindring ikke håndteret korrekt - KS
3	SUF	39.550,41	151,74	Vurderes at være fejlagtigt håndteret - SUF
4	SUF	32.585,57	120,00	Vurderes at være fejlagtigt håndteret - SUF
5	BUF	29.606,09	111,62	Sygdomsperiode er ikke indberettet - BUF
6	SOF	28.199,55	37,42	Vurderes at være fejlagtigt håndteret - SOF
7	SOF	27.977,55	106,33	Overførsel ikke indberettet - SOF
8	SUF	27.129,21	125,24	Virksomhedsoverdragelse - KS
9	BUF	26.801,76	81,40	Vurderes at være fejlagtigt håndteret - BUF
10	SUF	26.029,16	102,05	Vurderes at være fejlagtigt håndteret - SUF
I alt		325.241,33	1.087,40	

Kilde: KS oversigt over afregning til Feriefonden 2023 med egen tilvirkning

Der henvises til afsnit 3.1 Nye bemærkninger og observationer 2024 omkring Afregning til Feriefonden.

5 Afslutning

De konstaterede forhold har været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

Yderligere spørgsmål eller kommentarer til rapporten kan rettes til EY, Ulrik B. Vassing på telefon 25 29 45 54 eller Intern Revision, Jesper Andersen på telefon 20 42 90 88.

København, den 12. december 2024
EY Godkendt Revisionspartnerselskab

Københavns Kommune

Ulrik B. Vassing
statsautoriseret revisor

Jesper Andersen
revisionschef

Rasmus F. Andersen
statsautoriseret revisor

6 Bilag 1 - Formidling af risiko og væsentlighed m.v.

Vi har i nærværende revision vurderet graden af risiko og væsentlighed for de enkelte observationer, og i tilknytning til den givne observation er påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med 🔴
▶ Prioritet 1-markeringer anvendes for forhold, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en revisionsbemærkning.
▶ Et forhold anses for kritisk, såfremt der er en høj grad af sandsynlighed for, at forholdet indtræffer og/eller har en betydelig effekt og/eller har en betydelig udbredelse.
▶ Prioritet 1-markeringer rapporteres til ledelsen med påkrav om, at disse forelægges for det stående udvalg eller Økonomiudvalget.
Prioritet 2 – markeres med 🟡
▶ Prioritet 2-markeringer anvendes for forhold, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre revisionsbemærkninger i årsberetningen.
▶ Et forhold anses for væsentlig, såfremt der er en middel grad af sandsynlighed for, at forholdet indtræffer og/eller har en vis effekt og/eller har en vis udbredelse.
▶ Prioritet 2-markeringer rapporteres til ledelsen i den reviderede forvaltning.
Prioritet 3 – markeres med 🟢
▶ Anvendes for forhold, der ikke har givet anledning til omtale eller kun anses for mindre væsentlige, og som derfor kun rapporteres til ledelsen som opmærksomhedspunkter.
▶ En risiko anses for mindre væsentlig, såfremt der er en lille grad af sandsynlighed for, at forholdet indtræffer og/eller har en lille effekt og/eller har en lille udbredelse.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jesper Gjøtterup Andersen
Revisionschef
På vegne af: Københavns Kommune
Serienummer: 068d0300-58d8-4d28-8673-0565d0fb9ff8
IP: 193.169.xxx.xxx
2024-12-12 12:20:14 UTC

Rasmus Friborg Andersen
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: e219fbda-f2e4-4cf2-b051-b646c7d11872
IP: 79.142.xxx.xxx
2024-12-12 12:45:36 UTC

Ulrik Benedict Vassing
EY Godkendt Revisionspartnerselskab CVR: 30700228
Statsaut. revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: 732cb4e7-8215-446a-997c-ab4b20a9363c
IP: 93.165.xxx.xxx
2024-12-12 13:51:50 UTC