Københavns Kommune

Revision af generelle IT-kontroller 2023

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 2023 har vi foretaget revision af generelle it-kontroller, som understøtter kommunes regnskabsaflæggelse.

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 udførelse af forretningsaktiviteter i brugersystemerne.

Københavns Kommune har aftale med KMD omkring drift af Kvantum, KMD Opus Debitor & 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 & KMD Opus Løn. For så vidt angår KY og KSD-applikationerne modtages der også årligt specifikke erklæringer. Revisionserklæringerne forventes modtaget i Q1 2024 dækkende 2023.

Afrapporteringen på gennemgangen af generelle it-kontroller relateret til Kvantum, KMD Opus Debitor og KMD Opus Løn afrapporteres i "Revisionsrapport – Regnskabsføring, forretningsgange og interne kontroller 2023", hvortil der henvises.

Forvaltningsrevision

Forvaltningsrevisionen har omfattet følgende områder:

- Ledelsestilsyn med brugerautorisationer
- Ibrugtagning af it-systemer (opfølgning på tidligere observationer)
- Leverandørstyring - outsourcing (opfølgning på tidligere observationer)
- Risikovurderinger af it-systemer (opfølgning på tidligere observationer)
- Organisering af informationssikkerhed og styrkelse af ISMS (opfølgning på tidligere observationer)
- BUF IT-drift (opfølgning på tidligere observation).

1.3 Revisionsarbejdets udførelse

Revisionen er udført på grundlag af godkendt revisionsplan for 2023, 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").

Afrapporteringen på gennemgangen af generelle it-kontroller relateret til Kvantum, KMD Opus Debitor og KMD Opus Løn afrapporteres i "Revisionsrapport – Regnskabsføring, forretningsgange og interne kontroller 2023", hvortil der henvises.

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 cyber-angreb eller andre alvorlige it-sikkerhedsmæssige hændelser, er tilsvarende stigende. KK har derfor behov for løbende at vurdere tilstrækkeligheden af de etablerede sikringsforanstaltninger, herunder sikre, at der er et ledelsessystem med tilstrækkelige kompetencer, ressourcer og uafhængighed på informationssikkerhedsområdet.

Kommunens tidligere revision Deloitte har i 2021 og 2022 haft drøftelser med Koncern IT (KIT) vedrørende den nuværende organisering på informationssikkerhedsområdet samt planer for styrkelse af informationssikkerheden og det ledelsessystem, der understøtter dette.

I forlængelse heraf er der nedsat et projekt "Et styrket ISMS" og tilknyttet en styregruppe.

Vi har noteret os, at status på dette arbejde i oktober 2023 er følgende:

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

Vi har fået oplyst, at der er udarbejdet en analyse, hvor der er identificeret, hvilke elementer, der fungerer tilfredsstillende i forhold til et velfungerende ISMS, samt identificeret behov for nødvendige tiltag, der sikrer et velfungerende ISMS, der er passende for en organisation og et it-miljø af KKs størrelse og kompleksitet.

Vi har noteret os, at GAP analysen vil være grundlaget for, at styregruppen kan beslutte videre arbejde med et styrket ISMS i Københavns Kommune.

Det videre arbejde forventes blandt andet at omfatte initiativer i forhold til løbende rapportering på informationssikkerhedsområdet samt en dokumenteret vurdering af, hvilke af ISO 27002's foreslåede kontroller, der er relevante at implementere (dokumenteret i et SoA-dokument). Sammen med risikovurderingen vil SoA ("Statement of Applicability") dokumentet danne grundlag for at planlægge, udføre, kontrollere og kontinuerligt forbedre informationssikkerheden.

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

Vi noterer os, at GAP analysen har identificeret, at der var behov for at sikre passende ressourcer med de nødvendige kompetencer og den nødvendige uafhængighed til at styrke tilsynet med informationssikkerhed i KK. Der er fortsat behov for at etablere en effektiv tilsynsfunktion.

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. Vi har i forbindelse med revisionen indhentet og gennemgået udvalgte risikovurderinger, ligesom vi har drøftet processen for udarbejdelse af risikovurderinger generelt.

Vi har noteret os, at risikovurderinger af systemer ikke foretages 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.

De nuværende risikovurderinger af systemer bør styrkes, således at 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 arbejder på at ændre risikovurderingsmetoden til at være mere baseret på en egentlig vurdering af risici på baggrund af opdaterede trusselsvurderinger. På tidspunktet for vores revision var denne tilgang dog endnu ikke implementeret i væsentligt omfang og omfattede kun meget få trusselsscenarier.

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 2023 har udført et stort arbejde med at få udarbejdet sikkerhedsvurdering af et stort antal systemer, i forlængelse af revisionens bemærkning herom fra 2022.

Vores opfølgning i 2023 har dog vist, at KK ikke er helt i mål med arbejdet i forhold til at sikre, at kommunens regler er efterlevet fuldt ud. Særligt er der mangler i forhold til systemer ibrugtaget før 1. november 2018. Umiddelbart er det vores vurdering, at risikoen alt andet lige er større på ældre systemer. Det er ledelsens ansvar, at der ikke foretaget sikkerhedsvurdering af systemer ibrugtaget før 2018.

Ledelsestilsyn med brugerautorisationer

Det fremgår af cirkulæret for informationssikkerhed, at der for alle systemer, der ikke er integreret i IGA (Identity Governance & Administration), skal udføres ledelsestilsyn minimum hver 6 måned.

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

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

En stikprøvevis gennemgang har vist, at ledelsestilsyn med autorisationer i flere tilfælde, ikke 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.

For at minimere omfanget af manuelle ledelsestilsyn kan organisationen bl.a. udarbejde medarbejderprofiler, som giver adgang til en "samlet" system portefølje, som er nødvendig for, at medarbejderen kan udføre sin rolle. Ledelsestilsynet bliver således afgrænset til at revidere rollerne. Det er en forudsætning, at der for de enkelte systemer er udarbejdet saglige roller og rettighedstildelinger.

Det er således det samlede kontrolmiljø der skal sikre, at kommunens styring er effektiv, og ikke det enkelte ledelsestilsyn.

Leverandørstyring

Kommunens tidligere revision Deloitte har i 2021 og 2022 haft fokus på processen vedrørende leverandørstyring, særligt processen for it-anskaffelser samt ansvarsfordeling og retningslinjer for leverandørstyring, herunder processer og retningslinjer for løbende overvågning af leverandører fx.

- Modtagelse af erklæring
- SLA-rapportering
- Møder med leverandør
- Spørgeskemaer til leverandør
- El.lign.

Det er tidligere anført, at KIT initierede en intern analyse på tværs af alle forvaltninger i Københavns Kommune i 2020. Formålet var at belyse systemejerrollen i Københavns Kommune. Analysen mundede ud i 8 hovedobservationer, hvor særligt én har haft betydning for revisionen, herunder H7 - *utilstrækkelig styring af kontrakter og leverandører på det enkelte it-system*.

Det er aftalt med ledelsen i KIT, at processer for opfølgning og risikovurdering af leverandører og de services, der leveres, samt overvågning af leverandører indgår som en del af kommunens fremtidige ISMS.

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 for 2023

Forvaltning	Forvaltningerne	Revisionsområde	Brugerautorisationer/IGA/IAM	Væsentlighedsniveau
Reference	3.1.1	Revisionsemne	Ledelsestilsyn med bruger autorisationer	
Observation	*Ledelsestilsyn med bruger autorisationer* Det fremgår af cirkulæret for informationssikkerhed, at alle systemer, der ikke er integreret i IGA (Identity Governance & Administration), skal udføre ledelsestilsyn minimum hver 6 måned. For systemer integreret i kommunens IGA-løsning inddeles systemer efter kritikalitet, hvor der henholdsvis skal udføres tilsyn, minimum hvert år eller hvert andet. Af kommunens systemregister fremgår det, at der er et stort antal systemer, der behandler personoplysninger. Af disse er 245 systemer integreret i IGA. Der er udtaget 25 stikprøver på systemer i IGA, hvor der er fastsat en frist for ledelsestilsyn og 25 for de systemer, hvor der ikke er fastsat frist. Alle de udvalgte systemer behandler følsomme personoplysninger jf. FISKK. I flere tilfælde var der jf. oplysningerne i IGA-løsningen ikke udført eller påbegyndt et ledelsestilsyn.			2023
Revisionsbemærkning	Det henstilles, at de ledelsestilsyn som skal sikre at de ansatte ikke har adgang til personoplysninger, hvor der ikke er et arbejdsbetinget behov, udføres i overensstemmelse med kommunens regler. Det gælder både de systemer, der er integreret i IGA-løsningen, og med stor sandsynlighed også de systemer, der ligger uden for IGA-løsningen. Det anbefales, at ledelsestilsynene for systemer integreret i kommunens IGA-løsning opstartes automatisk. Det henstilles desuden at alle kommunens systemer indeholdende værdi og personoplysninger, hvis det er teknisk muligt, integreres i kommunens IGA-løsning.			

3.2 Videreførte bemærkninger og observationer fra tidligere år

<table>
<tr><td>Forvaltning</td><td>ØKF</td><td>Revisionsområde</td><td>Ibrugtagningstilladelser på it-systemer</td><td rowspan="2">Væsentlighedsniveau</td></tr>
<tr><td>Reference</td><td>3.2.1</td><td>Revisionsemne</td><td>Ibrugtagning af it-systemer</td></tr>
<tr><td>Observation</td><td colspan="3">
Observationen er foretaget af Deloitte, der på tidspunktet for konstateringen var kommunens eksterne revision.

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

En sikkerhedsvurdering tager stilling til, at alle krav til informationssikkerhed og databeskyttelse er opfyldt. På baggrund af sikkerhedsvurderingen udstedes en ibrugtagningstilladelse. It-systemer skal have en ibrugtagningstilladelse, inden de idriftsættes.

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

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

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

<table>
<tr><th>Status</th><th>Antal</th></tr>
<tr><td>Ibrugtagningstilladelse m. handleplan</td><td>41</td></tr>
<tr><td>Godkendt</td><td>17</td></tr>
<tr><td>Skal sikkerhedsvurderes ved væsentlige ændringer</td><td>17</td></tr>
<tr><td>Ikke godkendt</td><td>1</td></tr>
<tr><td>Udfaset</td><td>17</td></tr>
<tr><td>Planlagt udfaset</td><td>2</td></tr>
<tr><td>Total</td><td>95</td></tr>
</table>

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

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

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

I to tilfælde have systemet fået nye systemintegrationer, som jf. forretningscirkulæret for it-anskaffelser er en væsentlig ændring. Dette burde derfor have givet anledning til en sikkerhedsvurdering.
Der er 135 systemer, som er anskaffet før 1.november 2018, der ikke har en ibrugtagningsstatus.
</td><td>2023
2022</td></tr>
</table>

	Det er desuden konstateret, at der er 16 systemer, der har en "ikke godkendt" status. Systemerne ser forsat ud til at være i drift. Et system har været i drift siden 2011, mens de øvrige er taget i drift i perioden 2014-2018.	
Revisionsbemærkning	Det henstilles at de systemer der ikke har en ibrugtagningsstatus, bliver gennemgået og oplysningerne i FISKK bliver opdateret. Det henstilles desuden, at der udføres en tilpasset sikkerhedsvurdering af systemer ibrugtaget før 2018, som ifølge det oplyste først sikkerhedsvurderes, hvis der sker væsentlige ændringer. Umiddelbart er det vores vurdering at risikoen alt andet lige er større på ældre systemer. Det henstilles, at de systemer, der har status "ikke godkendt" eskaleres, jf. anskaffelsescirkulæret, og der træffes de nødvendige foranstaltninger bl.a. om udfasning, idet disse jf. kommunes regler udgør en sikkerhedsrisiko.	

Forvaltning	ØKF	Revisionsområde	ISMS	Væsentlighedsniveau
Reference	3.2.2	Revisionsemne	Organisering af informationssikkerhed og styrkelse af det ISMS	
Observation	*Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System).* Observationen er foretaget af Deloitte, der på tidspunktet var kommunens ekstern revision. På baggrund af de konstant stigende trusler på informationssikkerhedsområdet er der behov for løbende at vurdere tilstrækkeligheden af de etablerede sikringsforanstaltninger, herunder sikre, at der er et ledelsessystem med tilstrækkelige kompetencer, ressourcer og uafhængighed på informationssikkerhedsområdet. KK har nedsat et projekt med tilknyttet styregruppe, der har til formål at sikre et styrket ISMS. Dette omfatter blandt andet forbedring af risikovurderinger, implementering af relevante sikringsforanstaltninger og rapportering på informationssikkerhedsområdet. Yderligere vil organisering af informationssikkerhedsområdet ligeledes blive vurderet, herunder sikre passende ressourcer med de nødvendige kompetencer og den nødvendige uafhængighed til at overvåge informationssikkerheden. Status 2023 Der er blevet udarbejdet en GAP-analyse med henblik på at identificere mere specifikt, hvilke områder der skal styrkes. Der er desuden blevet nedsat en styregruppe og oprettet en projektorganisering, der skal håndtere processen i forhold til at styrke kommunens ISMS og håndtere de observationer, der er påpeget i GAP-analysen.			2023 2022

	Det er aftalt med ledelsen i KIT, at observationen omkring leverandørstyring indgår som en del af kommunes fremtidige ISMS, hvorfor observationen er indarbejdet i dette punkt, hvor følgende risiko blev noteret: "Manglende eller utilstrækkelig styring og monitorering af leverandører medfører risiko for, at de leverede ydelser ikke dækker forretningsmæssige behov, samt at leverandører ikke efterlever det forventede IT-sikkerhedsniveau."	
Revisionsbemærkning	Vi henstiller, at arbejdet med at styrke informationssikkerheden fortsat prioriteres højt, herunder at: ▶ Der med afsæt i den foretagne GAP-analyse identificeres, hvilke områder der skal styrkes ▶ Det vurderes, hvorledes organiseringen af informationssikkerhedsområdet bør være, så dette sikrer tilstrækkelige kompetencer og uafhængighed. Der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt. Vi henstiller, at der etableres en proces for opfølgning på leverandører som omfatter en risikovurdering af leverandøren og de services der leveres og på baggrund heraf og at der foretages en stillingtagen om hvorledes overvågningen af leverandøren skal foretages, eks. ▶ Modtagelse af erklæring ▶ SLA rapportering ▶ Møder med leverandør ▶ Spørgeskemaer til leverandør ▶ El.lign.	

Forvaltning	ØKF	Revisionsområde	Risikovurderinger	Væsentlighedsniveau
Reference	3.2.3	Revisionsemne	Risikovurderinger	
Observation	Observationen er foretaget af Deloitte, der på tidspunktet var kommunens ekstern revision. Risikovurderinger af systemer foretages ikke for alle systemer, men kun de systemer, der enten har været i drift i minimum fire år, eller hvor forvaltningen er usikker på, om informationssikkerhedsniveauet er tilstrækkeligt, samt for systemer, der anvendes tværgående i KK's forvaltninger. I forhold til de foretagne risikovurderinger har Deloitte noteret, at disse er baseret på en liste af "standard" kontrolområder. Der ligger ikke et egentlig opdateret trusselskatalog til grund for disse risikovurderinger. Ligeledes kunne de ikke, på baggrund af den foreliggende dokumentation, se, at der er konsekvent, der foretages en dokumenteret vurdering af, hvorvidt de mitigerende sikringstiltag og kontroller faktisk fungerer hensigtsmæssigt. Status 2023 Der arbejdes fortsat på et nyt risikovurderingskoncept baseret på egentligt trusselskatalog.			 2023 2022
Revisionsbemærkning	Vi henstiller, 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.			

3.3 Lukkede bemærkninger og observationer fra tidligere år

I 2023 er der lukket én væsentlig observation fra 2022:

- BUF IT-Drift – periodisk passwordskift: Det er påset, at Børn- og Ungeforvaltningen har fået implementeret periodisk passwordskifte pr. 2. oktober 2023 i forbindelse med udrulning af NSIS (National Standard for Identitets Sikring) for de pædagogiske medarbejdere på skoler og i dagtilbud.

I 2023 er en væsentlig observation fra 2022 overført til en anden væsentlig observation i 2023:

- Leverandørstyring - procedure og retningslinjer for leverandørstyring: Det er aftalt med ledelsen i KIT, at processer for opfølgning og risikovurdering af leverandører og de services, der leveres, samt overvågning af leverandører indgår som en del af kommunens fremtidige ISMS.

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 14. december 2023

EY

Ulrik B. Vassing

statsautoriseret revisor

Rasmus F. Andersen

statsautoriseret revisor

Københavns Kommune

Jesper Andersen

revisionschef

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 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.