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