Handleplaner vedr. Generelle IT-kontroller 2022

Bemærkninger i den løbende revision vedr. Generelle IT-kontroller 2022		
Nr. 3.1.1	Ibrugtagning af it-systemer	Økonomiforvaltningen
Nr. 3.1.2	Organisering af informations-sikkerhed og styrkelse af det ISMS	Økonomiforvaltningen
Nr. 3.1.3	Risikovurderinger	Økonomiforvaltningen
Nr. 3.2.1	Outsourcing-leverandørstyring	Økonomiforvaltningen
Nr. 3.2.2	BUF IT-drift	Børne- og Ungdomsforvaltningen

Revisionsbemærkning nr. 3.1.1 Ibrugtagning af it-systemer	
Farvemarkering (prioritet)	Rød
Gives til	Økonomiforvaltningen

Observationer og risici:
Ibrugtagningstilladelse
Den nye borgerserviceplatform i Kultur- og Fritidsforvaltningen (KFF), der anvendes til at udstede pas og kørekort, blev taget i brug d. 27. juli 2022 uden en ibrugtagningstilladelse.
KFF og KIT samarbejdede sideløbende om at bringe de tekniske og sikkerhedsmæssige udfordringer i orden. KIT orienterede i juli 2022 KFF om, at en ibrugtagningstilladelse ikke ville kunne gives inden borgerplatformen skulle idriftsættes den 27. juli 2022, da der ikke forelå en fyldestgørende handleplan for at håndtere de tekniske og sikkerhedsmæssige udeståender.
Den 2. september forelå en ibrugtagningstilladelse, som indeholdt en liste over 29 tekniske udeståender. KIT kan på det tidspunkt ikke udstede en officiel ibrugtagningstilladelse til systemet. KFF har efterfølgende udarbejdet en handleplan, der imødegår problemstillingerne, og Koncern IT har udstedt en betinget ibrugtagningstilladelse med handleplan d. 26. september 2022.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
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. Da KIT meddelte KFF, at en ibrugtagningstilladelse ikke ville kunne udstedes forud for idriftsættelsen, burde sagen derfor have været behandlet som uoverensstemmelse. Dette indebærer en eskalering til hhv. DCK og ITK, hvor der skal opnås enighed, hvis sagen ikke skal eskaleres yderligere til de relevante administrerende direktører, borgmestre og ultimativt til ØU. Det er forbundet med stor risiko for kommunen at idriftsætte et IT-system uden en sikkerhedsvurdering og en ibrugtagningstilladelse. Det henstilles, at forvaltningerne følger anskaffelsesprocessen, og Koncern IT følger eskalationsprocessen, hvis en tilsvarende sag opstår. Det henstilles samtidig, at KIT undersøger, om der er flere IT- systemer der er idriftsat uden at der foreligger en ibrugtagningstilladelse.	Økonomiforvaltningen

Handleplan januar 2023	Opfølgning
Økonomiforvaltningen - Af cirkulæret og forretningsgangene for it-anskaffelser fremgår det, at den anskaffende enheds direktion er ansvarlig for, at der bliver udarbejdet en sikkerhedsvurdering og gives en ibrugtagningstilladelse forud for idriftsættelse af it-systemer.	**Økonomiforvaltningen** - Handleplanen er udarbejdet og behandles efter planen af It-kredsen på mødet i januar 2023. - Handleplanen forventes gennemført inden udgangen af Q2 2023 og punktet forventes dermed at kunne lukkes inden næste revision (ultimo 2023).

Handleplan januar 2023	Opfølgning
- KIT vil internt sikre, at eskalationsprincippet følges ved uoverensstemmelse mellem KIT og en projektejende forvaltning. - Arbejdet koordineres af Koncern IT med reference til It-kredsen og vil føre til en fælles handleplan, der inden næste revision skal sikre, at der for alle relevante systemer i drift foreligger ibrugtagningstilladelser. Handleplanen vil indeholde en prioritering af hvilke systemer, der skal vurderes først. Det bemærkes, at alle forvaltninger som følge af den nævnte sag har igangsat tiltag for at få sikkerhedsvurderet it-systemer, der ikke har fået ibrugtagningstilladelse.	Fremdriften på handleplanen monitoreres løbende, og der gives status til It-kredsen hvert kvartal, 2023

Revisionsbemærkning nr. 3.1.2 Organisering af informationssikkerhed og styrkelse af det ISMS	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen

Observationer og risici:
Organisering af informationssikkerhed i Københavns Kommune og styrkelse af det etablerede ISMS (Information Security Management System).
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 erkendt behovet herfor og har nedsat et projekt med tilknyttet styregruppe, der har til formål at sikre et styrket ISMS.

Det er vores forståelse, at projektet vil arbejde med styrkelse af ledelsessystemet for informationssikkerhed baseret på ISO 27001 (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.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller, at arbejdet med at styrke informationssikkerheden prioriteres højt, herunder at der: • Foretages en GAP-analyse af det nuværende ISMS med henblik på at identificere mere specifikt, hvilke områder der skal styrkes • Med afsæt heri vurderes, hvorledes organiseringen af informationssikkerhedsområdet bør være, således at dette sikrer tilstrækkelige kompetencer og uafhængighed • Der sker en dokumenteret opfølgning på, at etablerede sikringstiltag og kontroller fungerer hensigtsmæssigt.	Økonomiforvaltningen

Handleplan januar 2023	Opfølgning
Økonomiforvaltningen - Københavns Kommune har som følge af anbefalingen fra tidligere år igangsat et arbejde, der skal føre til etableringen af et ISMS i Økonomiforvaltningen. Arbejdet følger den aftalte tidsplan - Konkret vil der blive udarbejdet en GAP-analyse med anbefalinger, tilpasninger og	**Økonomiforvaltningen** - Handleplanen forventes gennemført inden næste revision (ultimo 2023) - GAP-analysen der skal resultere i anbefalede indsatser for styrkelse af ISMS afsluttes i Q1 2023 - De anbefalede indsatser forelægges for relevante ledelsesfora til prioritering og godkendelse i Q2 2023

Handleplan januar 2023	Opfølgning
ændringer af Københavns Kommunes regler på informationssikkerhedsområdet	- Indsatser vedr. tilpasning af organiseringen på informationssikkerhedsområdet implementeres i Q3 2023 - Risikovurdering af Økonomiforvaltnings forretningsområde gennemføres i Q3 2023 - SoA-dokument implementeres i Q4 2023 Indsatser vedr. tilpasning af regler på informationssikkerhedsområdet implementeres i Q4 2023

Revisionsbemærkning nr. 3.1.3 Risikovurderinger	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen

Observationer og risici:
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.

I forhold til de foretagne risikovurderinger har vi noteret os, at disse er baseret på en liste af "standard" kontrolområder. Der ligger ikke et egentlig opdateret trusselskatalog til grund for disse risikovurderinger. Ligeledes kan vi ikke, på baggrund af den foreliggende dokumentation, se, at der er konsekvent, foretages en dokumenteret vurdering af, hvorvidt de mitigerende sikringstiltag og kontroller faktisk 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.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller, at: • De nuværende risikovurderinger af systemer styrkes, således at 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	Økonomiforvaltningen

Handleplan januar 2023	Opfølgning
Økonomiforvaltningen - Revisionen henstiller, at risikovurderingskonceptet styrkes og udvides, så det i højere grad tager afsæt i trusselsvurderingerne mod Københavns Kommune For at imødekomme dette er det i koordination med Københavns Kommunes DPO aftalt og godkendt i It-kredsen i november 2022, at Økonomiforvaltningen udarbejder et nyt koncept for risikovurderinger, der samler it-systemvurderingerne med gdpr-vurderingerne mest hensigtsmæssigt.	**Økonomiforvaltningen** - Handleplanen forventes gennemført i februar 2023 - Økonomiforvaltningen har i samarbejde med Københavns Kommunes DPO igangsat arbejdet med et nyt risikovurderingskoncept for kommunen. Det er aftalt, at det nye koncept præsenteres for Digitaliseringschefkredsen og It-kredsen januar 2023 Det er videre aftalt, at Økonomiforvaltningen samtidig (januar 2023) præsenterer de to kredse for en handlingsplan, der skal beskrive, hvordan arbejdet med risikovurderinger generelt skal organiseres i Københavns Kommune, herunder særligt hvordan Koncern IT vil organisere sig og sikre den nødvendige dimensionering af opgaven.

Revisionsbemærkning nr. 3.2.1 Outsourcing-leverandørstyring	
Farvemarkering (prioritet)	Gul
Gives til	Økonomiforvaltningen

Observationer og risici:
Outsourcing- anskaffelsesprocedure og retningslinjer for leverandørstyring
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.
Vi har konstateret, at IT-anskaffelser og kontraktindgåelser for ældre systemer ikke følger Københavns Kommunes Governance-model herfor.
Yderligere har vi konstateret, at der ikke foreligger klare retningslinjer for leverandørstyring, som er gældende på tværs af alle forvaltninger.
Processen er forankret i de enkelte forvaltninger, hvilket gør, at monitorering og opfølgning ikke sker i tilstrækkelig grad.
Status 2022
Vi har fået oplyst, at Københavns Kommune med DCK som styregruppe har igangsat forbedrende tiltag i form af implementering af værktøjer og metoder med henblik på at konkretisere og operationalisere systemejerrollen, herunder i forhold til leverandørstyring.
Ligeledes igangsættes arbejder med henblik på at forbedre IT-kontraktstyringen på tværs af forvaltningerne.
Punket opretholdes og forventes lukket ved revisionen af 2023.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller, at leverandørkontrakter undergår Københavns Kommunes Governance-model ved genforhandling. Derudover henstiller vi, at der etableres fælles administrative forretningsgange for opfølgning.	Økonomiforvaltningen

Handleplan januar 2023	Opfølgning
Økonomiforvaltningen - Økonomiforvaltningen vil udvide den nuværende forretningsgang for it-anskaffelser med en forretningsgang for opfølgning på leverandørkontrakter, alternativt udarbejde en ny forretningsgang herfor - Herudover er der igangsat en indsats for at konkretisere og operationalisere systemejerrollen i forhold til leverandørstyring. - Indsatsen koordineres med de generelle indsatser for at professionalisere systemejerområdet i Københavns Kommune, hvor der arbejdes på et årshjul for systemejeropgaver, der vil understøtte systemejerne og de systemansvarlige chefers mulighed for kontrol af gennemførelse af opgaverne I forlængelse heraf vil Økonomiforvaltningen foreslå en investeringscase til Budget 24 med henblik på konkret understøttelse af forvaltningerne i opgaven, herunder implementering af forretningsgangen.	**Økonomiforvaltningen** - Udarbejdelse af forretningsgang for opfølgning på leverandørkontrakter igangsættes Q2 2023 og forventes klar til behandling i It-kredsen Q3 2023 og implementering Q4 2023 - Indsatsen for at konkretisere og operationalisere systemejerrollen i forhold til leverandørstyring er igangsat i et samarbejde på tværs af forvaltningerne. Det er forventningen, at udmøntningen af arbejdet kan ske Q3-4 2023 Budgetsagen, der skal sikre midler til yderligere tiltag indenfor området, udarbejdes Q1-2 frem mod budgetforhandlingerne Q3 2023

Revisionsbemærkning nr. 3.2.3 BUF IT-drift	
Farvemarkering (prioritet)	Gul
Gives til	Børne- og Ungdomsforvaltningen

Observationer og risici:

BUF IT-drift
Vi har konstateret, at der ikke er opsat tvunget periodisk skift af password for brugere, som tilgår BIT's AD, baseret på Københavns Kommunes generelle krav til passwordpolitik.
Vi er oplyst om, at denne forventes implementeret i forbindelse med implementeringen af den nye nationale standard NSIS, hvor BUF IT-drift er en del af NSIS-projektet.
Status 2022
Vi har fået oplyst, at forholdet er uændret.
NSIS-løsningen forventes implementeret primo 2023.
Punktet opretholdes og forventes lukket ved revisionen af 2023.

Revisionsbemærkning:	**Berørt(e) forvaltning(er):**
Vi henstiller, at der arbejdes videre med implementeringen af periodisk passwordskift, således at løsningen bliver underlagt det ønskede IT-sikkerhedsniveau, som er fastlagt af Københavns Kommune.	Børne- og Ungdomsforvaltningen

Handleplan januar 2023	**Opfølgning**
Børne- og Ungdomsforvaltningen **Primo 2023:** Frivilligt password-skift implementeret **Marts 2023:** NSIS-løsning inkl. tvungent password-skifte implementeret for alle medarbejdere **Marts 2023:** NSIS-revisionsrapport udarbejdet	**Børne- og Ungdomsforvaltningen** Alle medarbejdere vil via NSIS årligt blive afkrævet automatisk password-skifte.