Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C

Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

Københavns Kommune
Økonomiforvaltningen
Att.: Direktionen
Rådhuspladsen 1
1550 København V

It-sikkerhedsarbejdet på udvalgte områder i Københavns Kommune

Indledning

Deloitte har i 2016 efter aftale med Københavns Kommune foretaget en opfølgning på sidste års observationer, baseret på følgende:

- Overordnet interview med kommunens it-sikkerhedsansvarlige kontorchef og gennemgang af enkelte udvalgte kontroller i KIT som opfølgning på vores notat af 19. januar 2016 vedrørende cybersikkerhed og compliance med persondataloven (data privacy) samt
- Indhentet, opdateret status på vurdering af kommunens modenhedsniveau inden for informationssikkerhed, jf. de områder, der er defineret i ISO/IEC 27001. Kommunen har i 2016 iværksat en opdatering af den i 2014 gennemførte modenhedsmåling på informationssikkerhedsområdet, gennemført af et eksternt sikkerhedskonsulentfirma.

Rapporteringen er opbygget på følgende måde:

1. Formål og omfang mv.
2. Ledelsesresume og konklusion
3. Observationer, risikovurdering og anbefaling
4. Organisatoriske forhold omkring it-sikkerhed mv.
5. Formidling af risiko og væsentlighed mv.

1. Formål, omfang mv.

1.1 Undersøgelsens formål

Formålet med nærværende undersøgelse har været at følge op på de væsentlige it-risici, som er blevet adresseret under sidste års gennemgang, og som relaterer sig til andre områder end regnskabsaflæggelsen, herunder f.eks. at berøre andre områder som f.eks. cybersikkerhed og data privacy med henblik på at identificere, om kommunens prioriteringer og igangværende tiltag inden for de nævnte områder på overordnet niveau anses for tilstrækkelige.

1.2 Undersøgelsens omfang og afgrænsning

Vi har ifølge aftale med Københavns Kommune tidligere udvalgt 10 nøglekontroller, alle fokuseret omkring it-sikkerhed og beskyttelse af persondata i forretningsprocesserne, og forespurgt til Københavns Kommunes arbejde med opretholdelsen af disse kontroller, herunder kontroller ift. anvendelse af serviceleverandører og generel ledelsesmæssig styring og opfølgning, som vi i 2016 har foretaget en opfølgning på.

Vi har i nærværende rapport opsummeret de forhold, som har givet anledning til bemærkninger, og som vi har fået oplyst i forbindelse med ovenstående gennemgang.

1.3 Undersøgelsens udførelse

Opfølgningen på de udvalgte kontroller samt på risikovurderingsprojektet er gennemført som interviews og gennemgang af modtaget materiale. Vi har ikke foretaget revision.

Vores opfølgning er i udstrakt grad baseret på den modenhedsvurdering af informationssikkerhed, som Københavns Kommune har foranlediget gennemført i 2016 ved brug af eksterne sikkerhedskonsulenter. Modenhedsvurderingen er foretaget af de 15 områder inden for informationssikkerhed, der er fastlagt i ISO 27001.

2. Ledelsesresume og konklusion

2.1 Persondataloven

På baggrund af vores opfølgning på sidste års gennemgang er det vores vurdering, at der i al væsentlighed fortsat er designet retningslinjer for sikring af persondata i KIT, herunder, at data er klassificeret. Vi har ikke haft mulighed for at verificere, om disse er implementeret i de enkelte forvaltninger.

Vi er bekendt med at kommunen har bevilliget betragtelige midler og nedsat flere organer med henblik på at opnå samlet compliance med den kommende persondataforordning.

2.2 Cybersikkerhed

Det er vores opfattelse, at arbejdet med implementering af en fælles risikostyringsmodel også i 2016 fortsat er i fokus og i fremdrift. Det konstateres i den eksterne modenhedsvurdering, at der er sket en

lille stigning i modenhedsniveauet med 0,6. En væsentlig forklaring herpå bunder i, at der nu er implementeret en risikovurderingsmetodik i KIT, som benyttes ved risikovurdering af it-infrastruktur. Metodikken er dog ikke operationaliseret og endnu ikke implementeret i hele KK, f.eks. i de enkelte forvaltninger. Der er konstateret et væsentligt øget fokus på metode, hvilket var et væsentligt kritikpunkt i 2015.

Københavns Kommune har igangsat tiltag ved at implementere en "end-to-end process" som skal sikre, at stillingtagen til risikovurderingerne bliver taget med i et årshjul. Der vil endvidere blive udarbejdet en klar opgave-/ansvarsplacering. Målet med disse tiltag er, at der i fremtiden skal kunne opstilles et samlet risikobillede for hele Københavns Kommune.

Den i 2015-rapporten omtalte logovervågningsløsning (SIEM) er fortsat ikke fuldt implementeret for basissystemer. Vi har dog fået oplyst, at der er implementeret en procedure, hvor væsentlige sikkerhedshændelser behandles i "ledelsesforum for it-sikkerhed", som bl.a. indeholder afrapporteringsmøder, hvor drøftelser skal foregå ud fra en konkret oversigt over de hændelser, der har været. På baggrund heraf vil der ske en konsolideret rapportering.

I forhold til oplysninger på bærbare pc'er har vi konstateret, at der er implementeret en procedure for bortskaffelse af harddiske, samt at der er igangsat et projekt, hvor operativsystemer opgraderes, og i den forbindelse vil harddiske blive krypteret. For retningslinjer for brug af de mobile enheder såsom smartphones og tablets er dette forhold udbedret ultimo august 2016.

2.3 ISO 27001 modenhedsanalyse

Status på forholdet omkring manglende central styring af leverandøradgange er, at der nu er etableret konkrete retningslinjer for tildeling og styring på leverandøradgange, men processen i forhold til en løbende ledelsesmæssig opfølgning på, hvorvidt leverandørerne overholder de sikkerhedskrav, som er stillet af Københavns Kommune, er endnu ikke på plads. Der er etableret et formelt ledelsestilsynskommissorium og forum for it-sikkerhed inden for området.

2.4 Status på it-risikostyring

Ledelses- og styringselementerne er efter vores vurdering det vigtigste at få designet og implementeret forud for implementering af de tekniske it-sikkerhedsløsninger, for ellers er der risiko for, at de tekniske it-sikkerhedsløsninger ikke implementeres effektivt i organisationen. Vi har i 2015 påpeget, at korrekt placering af roller og ansvar for it-sikkerhedsarbejdet i kommunen ville være afgørende for at kunne designe og implementere tilfredsstillende kontrolforanstaltninger i den videre proces. Kommunen har set på dette forhold med stor alvor og i løbet af 2016 investeret et stort antal ressourcer i at etablere det fornødne "ledelsesrum" for at kunne eksekvere den ønskede plan, ligesom der er søgt tillægsbevillinger til området. Dette kan efter vores opfattelse ikke direkte måles direkte i den kvantitative tilgang, hvormed den gennemførte modenhedsmåling på informationssikkerhedsområdet fra det eksterne sikkerhedskonsulentfirma er udført. Det ønskede modenhedsniveau er 4 på en skala fra 1 – 5, hvor det nuværende modenhedsniveau i målingen vurderes at være 2,3 mod tidligere 1,7.

Endvidere er der i forbindelse med vores gennemgang, jf. afsnit 3, konstateret en række svagheder omkring opbevaring af persondata samt styring og opfølgning på leverandørens systemadgange, hvor der fortsat ikke fuldt er implementerede løsninger herfor.

Efter det oplyste skal der for begge områder udføres yderligere tiltag for at højne sikkerheden på områderne. Vi har konstateret, at der i budgettet for 2017 er ansøgt om yderligere bevillinger til området.

Forvaltningens iværksatte tiltag	Vi har efter aftale ikke foretaget gennemgang af de af forvaltningen beskrevne tiltag, jf. nedenstående, men vil følge op herpå i forbindelse med revision af 2017.
	2015 - Ny handlingsplan og forslag om ny tilsynsfunktion På baggrund af revisors observationer og anbefalinger vil Økonomiforvaltningen (1) fremlægge en indstilling for Økonomiudvalget om en handlingsplan for øget rådgivning og støtte til forvaltningernes arbejde med it-sikkerhed og (2) herudover fremlægge en indstilling om, at der (jf. kommentar til pkt. 2.4. ovenfor) i forbindelse med implementering af den nye EU-forordning om persondata etableres en særlig ny tilsynsfunktion, placeret i Intern Revision. Ad (1): Handlingsplanen vil blive baseret på, at arbejdsdeling i den gældende it-sikkerhedspolitik videreføres, dvs. at forvaltningerne fortsat har ansvaret for, at der gennemføres risikovurderinger og ledelsestilsyn inden for forvaltningernes ansvarsområder, men KIT vil levere yderligere complianceredskaber og udbygget, konkret rådgivning til forvaltningerne. Handlingsplanen vil indeholde forslag om, at It-sikkerhedsfunktionen i KIT udbygges med yderligere ressourcer til at varetage disse opgaver. Handlingsplanen vil blive foreslået iværksat snarest muligt. Ad (2): Økonomiforvaltningen forventer, at det i løbet af 1. halvår 2016 bliver afklaret, præcis hvordan den nye EU-forordning skal implementeres i Danmark. Det er dog allerede klart, at der vil være krav om, at der etableres en ny funktion som databeskyttelsesansvarlig, der skal sikre, at organisationen lever op til lovgivningen på området. Økonomiforvaltningen vil fremlægge indstilling til Økonomiudvalget om etablering af en sådan ny funktion med virkning fra 2017. **2016** **Ad 1.** BR besluttede i forbindelse med Budget 2017 på baggrund af indstilling fra ØKF, at de beskrevne tiltag gennemføres. **Ad 2.** BR besluttede i forbindelse med Budget 2017 på baggrund af indstilling fra ØKF, at de beskrevne tiltag gennemføres.

3. Observationer, risikovurdering og anbefaling

3.1 Oversigt over observationer

Vi har som opfølgning på tidligere års observationer gennemgået de udvalgte ISO27001-kontroller og anført de detaljerede observationer og anbefalinger, som gennemgangen har givet anledning til, samt en status på risikostyringsprojektet. Vi har for de områder, der er relevante i forbindelse med vores gennemgang, tillige anført kommunens egne observationer.

Organisationsområde i Københavns Kommune	KIT	**Område/ emne**	Kontroller relateret til persondataloven

Ref.	**Observation**	**Kontrolområde og kontrolspørgsmål/risikobeskrivelse**	**Anbefaling/vurdering**	**Risiko og Væsentlighed**
Gennemgang af kontroller relateret til persondataloven				
A.1 Retningslinjer for sikkerhedsorganisationen	Vi har fået oplyst, at Københavns Kommune i samarbejde med PWC har foretaget en modenhedsanalyse, som har resulteret i en risikostyringsmodel, der beskriver de aktiviteter, som skal udføres for at skabe et samlet risikobillede. Vi har fået oplyst, at risici i forhold til kritiske aktiver i netværket, hvor KIT har ansvaret, er identificeret, og at næste step er at identificere risici i forhold til de enkelte forvaltninger. Projektet forventes afsluttet ultimo 2015. Vi har endvidere gennemgået den udleverede status på projektet inkl. aktuel tidsplan og har konstateret, at projektet er forsinket. **Status november 2016** Projektet kører fortsat og er i fremdrift, men ikke afsluttet på nuværende tidspunkt. KIT har fået tilført yderligere ressourcer.	**A.1 Retningslinjer sikkerhedsorganisation** Målsætning: At der foreligger en ledelsesgodkendt it-risikovurdering. **Kontrolspørgsmål:** Er følgende defineret: • Er trusler, der kan påvirke kommunens data og IT-systemer, vurderet? • Hvor ofte og af hvem opdateres risikovurderingen? • Hvordan indføres opdateringer og godkendelser?	Vi anbefaler, at risici i forhold til de enkelte forvaltninger identificeres, samt at der udarbejdes handlingsplaner for de identificerede risici. Endvidere skal vi anbefale, at der i forvaltningerne løbende allokeres tilstrækkelige ressourcer til projektet, såvel ledelsesmæssigt som udførende, for at sikre den videre fremdrift.	
A. 12 Retningslinjer for sikring af eksterne kommunikationslinjer er udarbejder	Vi har fået oplyst, at al kommunikation ud af huset, herunder datalinjer samt eksterne linjer til leverandører, er krypteret. Der er udarbejdet instrukser til brugen af sikre linjer, og vi har fået oplyst, at it-sikkerhedsafdelingen har medvirket i udarbejdelsen som led i det generelle it-sikkerhedsarbejde.	**A. 12 Retningslinjer kommunikation** Målsætning: At sikre, at ekstern kommunikation følger retningslinjer. **Kontrolspørgsmål:** Er der defineret og dokumenteret retningslinjer for ekstern kommunikation, herunder kommunikation mellem afdelinger og kommunikation med eksterne parter, eksempelvis via mail?	Ingen bemærkninger.	

Organisationsområde i Københavns Kommune	KIT	Område/ emne	Kontroller relateret til persondataloven

Ref.	Observation	Kontrolområde og kontrolspørgsmål/risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed
A. 14 Medarbejdere instrueres om, hvorledes behandling af data skal ske	Vi har fået oplyst, at alle medarbejdere er omfattet af tavshedspligt. I forbindelse med ansættelser instrueres medarbejderne i og gøres opmærksomme på relevante forhold vedrørende kommunens sikkerhedspolitikker, som er tilgængelige på kommunens intranet. Derudover gøres brugere løbende opmærksomme på, at de er med til at sikre datasikkerhed. Dette gøres løbende via interne kampagner.	**A. 14 Behandling af data** Målsætning: At der foreligger godkendte retningslinjer for medarbejdernes håndtering af persondata. **Kontrolspørgsmål:** Er der defineret og dokumenteret retningslinjer for, at alle medarbejdere, der skal arbejde med jobformidling, instrueres om gældende retningslinjer?	Ingen bemærkninger.	

Forvaltningens iværksatte tiltag	
	Vi har ikke foretaget revision af de af forvaltningen beskrevne tiltag, jf. nedenstående, men vil følge op herpå i forbindelse med revision af 2017.
	2015 - Ad A1. Retningslinjer for sikkerhedsorganisationen. KS er enig i anbefalingerne og har allerede tidligere i 2015 afsat de nødvendige ressourcer til opfølgning på opgaven. Jf. It-sikkerhedsregulativet er det forvaltningernes ansvar at foretage en risikovurdering inden for forvaltningens område, og det er KS' ansvar at stille de rette værktøjer og processer til rådighed for forvaltningerne. Implementering af opgaven i forvaltningerne forudsætter, at der også her afsættes de nødvendige ledelsesmæssige og personalemæssige ressourcer. KS vurderer, at processen i forhold til forvaltningerne kan gennemføres inden udgangen af 1. halvår 2016, såfremt forvaltningerne også afsætter de nødvendige ressourcer til opgaven. **2016** **Ad 1 risikovurdering.** BR vedtog i forbindelse med budgetforhandling 2017, at KIT overtager ansvaret for at gennemføre risikostyringsprocesser i forvaltningerne pr. 1. januar 2017 og sikrer, at der løbende foretages opfølgning på baggrund af et årshjul. KIT IT-sikkerhed har i samarbejde med forvaltningerne udarbejdet End-to-end process, herunder værktøjer og årshjul samt model for risikovurderinger i KK. Endvidere risikovurderingsmodel i forbindelse med ad hoc-vurderinger, f.eks. i forbindelse med it-anskaffelser mv. Proces iværksættes primo 2017 i nyt centralt it-risikoanalyseteam, så snart ansættelse af medarbejdere til risikoteam er tilendebragt. Der iværksættes i februar en betatest af proces og værktøjer i samarbejde med BIF med efterfølgende udrulning af proces til resterende forvaltninger. Erfaringer i forbindelse med implementering af risikovurderingsproces vil løbende blive indarbejdet med henblik på løbende forbedring og optimering af proces og tilhørende værktøjer.

Organisationsområde i Københavns Kommune	KIT	Område/emne	Kontroller relateret til cybersecurity

Ref.	Observation	Kontrolområde og kontrolspørgsmål/ risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed
Gennemgang af kontroller relateret til cybersecurity				
1. Risikovurdering	Vi har fået oplyst, at Københavns Kommune i samarbejde med PWC har foretaget en modenhedsanalyse, som har resulteret i en risikostyringsmodel, der beskriver de aktiviteter, som skal udføres for at skabe et samlet risikobillede. Vi har endvidere fået oplyst, at risici i forhold til kritiske aktiver i netværket, hvor KIT har ansvaret, er identificeret, og at næste step er at identificere risici i forhold til de enkelte forvaltninger. Projektet forventes afsluttet ultimo 2015. **Status november 2016** Projektet er i fortsat fremdrift, og den eksterne rapport påpeger, at der er målt en stigning i modenhedsniveauet med 0,6. Det er samtidig oplyst, at der er tilført yderligere ressourcer i form af 5 nye medarbejdere i KIT.	**Risikovurdering:** Målsætning: At sikre, at trusler er identificeret **Kontrolspørgsmål:** Er der defineret og dokumenteret retningslinjer for alle medarbejdere, der skal arbejde?	Vi henstiller til, at risici i forhold til de enkelte forvaltninger identificeres, samt at der udarbejdes handlingsplaner for de identificerede risici. Disse handlingsplaner bør forankres på et så tilstrækkeligt niveau i hver forvaltning, at der kan gennemføres en løbende ledelsesmæssig opfølgning på fremdriften. Endvidere skal vi anbefale, at der i forvaltningerne løbende allokeres tilstrækkelige ressourcer til projektet, såvel ledelsesmæssigt som udførende, for at sikre den videre fremdrift.	
2. Oplysning og uddannelse	Vi har fået oplyst, at roller og ansvar i forbindelse med kriseberedskab er defineret og kommunikeret til ledende medarbejdere. Vi har konstateret, at KIT har etableret et samlet It-beredskab, der også håndterer hændelser i forhold til cybersecurity, og at der løbende sker en revidering af processer og instrukser på baggrund af opsamling af erfaringer fra konkrete hændelser og øvelser.	**Oplysning og uddannelse:** Målsætning: At sikre den korrekte oplysning og uddannelse. **Kontrolspørgsmål:** Forstår ledende medarbejdere deres roller og ansvarsområder?	Ingen bemærkninger.	

Organisationsområde i Københavns Kommune	KIT	Område/emne	Kontroller relateret til cybersecurity

Ref.	Observation	Kontrolområde og kontrolspørgsmål/ risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed
Gennemgang af kontroller relateret til cybersecurity				
3. Datasikkerhed	Vi har fået oplyst, at datatransport for så vidt angår persondata og værdidata altid skal foregå ved krypteret trafik, og at data på fysiske diske og USB (beskyttet med password) sendes med personlig overdragelse, og der indhentes kvittering for modtagelse. Endvidere har vi observeret, at der ikke sker nogen systematisk opfølgning på, om medarbejdere i modstrid med reglerne opbevarer persondata på bærbare computere, og at data på disse computere ikke er krypteret. Endelig er det konstateret, at der hidtil ikke har foreligget retningslinjer for styring af mobile enheder (telefoner og tablet), men at sådanne retningslinjer, startende i oktober 2015, er under indførelse i forbindelse med det såkaldte "AirWatch-projekt". **Status november 2016** Vi har endvidere konstateret, at der er implementeret en procedure for bortskaffelse af informationsbærende medier, samt at der er igangsat et projekt, hvor Windows 7 skal udskiftes med Windows 10, og i den forbindelse vil harddiske blive krypteret ved hjælp af bitlocker. For mobile enheder er AirWatch etableret, og der er udarbejdet formelle retningslinjer.	**Data sikkerhed:** Målsætning: At sikre datasikkerhed for data i transit? **Kontrolspørgsmål:** Er data i transit beskyttet?	Vi har fået oplyst, at der arbejdes med etablering af tilsyn med, om der opbevares persondata på bærbare computere, og at det sikres, at alle data er hensigtsmæssigt beskyttet. Vi har dog fået oplyst, at IT-sikkerhedsfunktionen ikke har registreret sikkerhedshændelser, hvor data på bortkomne eller stjålne pc'er er blevet kompromitteret, men for at imødegå den potentielle risiko vil kommunen kryptere pc'er fremadrettet. Ligeledes oplyser kommunen, at alle udtjente pc'er destrueres for at sikre, at eventuelle data ikke kommer til uvedkommendes kendskab.	

Organisationsområde i Københavns Kommune	KIT	Område/emne	Kontroller relateret til cybersecurity

Ref.	Observation	Kontrolområde og kontrolspørgsmål/ risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed
Gennemgang af kontroller relateret til cybersecurity				
6. Sikkerhed kontinuerlig overvågning	Der er indgået kontrakt med eksterne leverandører, som løbende holder øje med netværkstrafikken og måler datamængder/trafikmængder. Vi har efterfølgende ved interview konstateret, at it-sikkerhedsafdelingen ikke hidtil har fulgt op på hændelser mv., idet processerne med overvågning har ligget uden for it-sikkerhedsafdelingen. Vi konstaterer, at der i oktober 2015 er indført rutiner, der skal sikre, at IT-sikkerhedsfunktionen får kendskab til alle it-sikkerhedshændelser, og at disse løbende afrapporteres til et nyetableret ledelsesforum for IT-Sikkerhed i KIT. Derudover har vi fået oplyst, at Københavns Kommune pt. er i gang med at implementere et logovervågningssystem på netværket. **Status november 2016** Københavns Kommune er fortsat i gang med implementeringen af en SIEM-løsning, som skal sikre en centraliseret logning for basissystemer og alarmering. Denne løsning er dog ikke fuldt implementeret endnu og omfatter kun udvalgte basissystemer. Det er endvidere oplyst, at sikkerhedsmæssige hændelser tages op i it-ledelsesforum.	**Sikkerhed kontinuerlig overvågning:** Målsætning: At sikre overvågning af netværk og fysisk miljø. **Kontrolspørgsmål:** Bliver eksterne serviceleverandørers aktiviteter overvåget for at afsløre potentielle hændelser relateret til cybersecurity?	Vi henstiller til, at KIT sikrer en fortsat udrulning af SIEM-løsningen til at omfatte basissystemer og øvrige systemer, hvor dette skønnes nødvendigt ud fra en risikobetragtning.	
Forvaltningens iværksatte tiltag	Vi har ikke foretaget revision af de af forvaltningen beskrevne tiltag, jf. nedenstående, men vil følge op herpå i forbindelse med revision af 2017.			

Organisationsområde i Københavns Kommune	KIT	Område/emne	Kontroller relateret til cybersecurity

Ref.	Observation	Kontrolområde og kontrolspørgsmål/ risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed

Gennemgang af kontroller relateret til cybersecurity

Ad 1 Risikovurdering.

KS er enig i anbefalingerne og har allerede tidligere i 2015 afsat de nødvendige ressourcer til opfølgning på opgaven. Jf. It-sikkerhedsregulativet er det forvaltningernes ansvar at foretage en risikovurdering inden for forvaltningens område, og det er KS' ansvar at stille de rette værktøjer og processer til rådighed for forvaltningerne. Implementering af opgaven i forvaltningerne forudsætter, at der også her afsættes de nødvendige ledelsesmæssige og personalemæssige ressourcer. KS vurderer, at processen i forhold til forvaltningerne kan gennemføres inden udgangen af 1. halvår 2016, såfremt forvaltningerne også afsætter de nødvendige ressourcer til opgaven.

Ad 3 Datasikkerhed.

KS er enig i anbefalingen. Det fremgår af de generelle instrukser vedr. IT-Sikkerhed, at der ikke må opbevares persondata på mobile enheder, og KS vil snarest udarbejde supplerende vejledning til forvaltningerne om, hvordan de kan opfylde deres driftsansvar på området. KS vil indarbejde tilsyn med forvaltningernes indsats på dette område i årsplan for tilsyn for 2016.

Mht. kryptering af data på bærbare pc'er har KS tidligere i 2015 anskaffet et produkt, som vil muliggøre kryptering på særligt udvalgte pc'er efter konkret bestilling. Yderligere vil data på alle bærbare pc'er blive krypteret i forbindelse med udrulning af nyt operativsystem (Windows 10).

IT-sikkerhedsfunktionen har ikke registreret sikkerhedshændelser, hvor data på bortkomne/stjålne pc'er er blevet kompromitteret, men for at imødegå den potentielle risiko tilbyder KS de omtalte løsninger vedr. kryptering. Det er tidligere besluttet, at IT-sikkerhedsfunktionen skal gennemføre en ny awarenesskampagne, særligt om, hvilke data der må opbevares på mobile enheder.

Alle udtjente pc'er destrueres for at sikre, at eventuelle data ikke kommer til uvedkommendes kendskab.

Økonomiforvaltningen anbefaler, at disse faktuelle informationer medtages i den endelige udgave af rapporten fra ekstern revision.

6 Sikkerhed kontinuerlig overvågning.

KS er enig i anbefalingen, og Økonomiforvaltningen anbefaler, at det indarbejdes, at anbefalingen om forankring af opfølgningen i It-sikkerhedsafdelingen er implementeret i oktober 2015, jf. den beskrevne observation.

2016

Ad 1 risikovurdering. - BR vedtog i forbindelse med budgetforhandling 2017, at KIT overtager ansvaret for at gennemføre risikostyringsprocesser i forvaltningerne pr. 1. januar 2017 og sikrer, at der løbende foretages opfølgning på baggrund af et årshjul.

KIT IT-sikkerhed har i samarbejde med forvaltningerne udarbejdet End-to-end process, herunder værktøjer og årshjul samt model for risikovurderinger i KK. Endvidere risikovurderingsmodel i forbindelse med ad hoc-vurderinger, f.eks. i forbindelse med it-anskaffelser mv.

Proces iværksættes primo 2017 i nyt centralt it-risikoanalyseteam, så snart ansættelse af medarbejdere til risikoteam er tilendebragt.

Der iværksættes i februar en betatest af proces og værktøjer i samarbejde med BIF med efterfølgende udrulning af proces til resterende forvaltninger.

Erfaringer i forbindelse med implementering af risikovurderingsproces vil løbende bliver indarbejdet med henblik på løbende forbedring og optimering af proces og tilhørende værktøjer.

KIT vil i forbindelse med gennemførelse af årshjul samt ad hoc-risikoanalyser ligeledes sikre, at der udarbejdes handlingsplaner for de identificerede risici, og forelægge disse for forvaltningsledelsen.

Ad 3 Datasikkerhed - KIT har i forbindelse med afklaringsmøder med Deloitte angivet, at KIT vil anbefale Intern revision, at der gennemføres tilsyn med, om der opbevares persondata på bærbare computere i forbindelse med it-tilsynsopgaven 2017.

Ad 6 Sikkerhed kontinuerlig overvågning - KIT arbejder målrettet for, at SIEM omfatter basissystemer og øvrige relevante systemer. Der arbejdes ud fra en liste af særligt kritiske fagsystemer, etableret i forbindelse med Legal Compliance, samt en række infrastrukturelementer.

Yderligere er der udarbejdet særlig "End-to-end process" for implementering af SIEM, som er under implementering februar 2017.

Implementering af SIEM er ligeledes i fokus i forbindelse med KIT's nye End-to-end process om risikostyring, ligesom SIEM altid indgår i overvejelser i forbindelse med anskaffelse af nye it-systemer.

Organisationsområde i Københavns Kommune	KIT	Område/emne	ISO 27001-kontroller	
Ref.	**Observation**	**Kontrolområde og kontrolspørgsmål/risikobeskrivelse**	**Anbefaling/vurdering**	**Risiko og Væsentlighed**
Gennemgang af udvalgte kontroller vedr. ISO 27001-kontroller				
A8. Styring af informationer	Vi har fået oplyst, at information og data er klassificeret efter lovmæssige krav, der er gældende for personoplysninger og Justitsministeriets bekendtgørelse om it-sikkerhed nr. 528. Derudover har vi fået oplyst, at data og information er klassificeret i 5 forskellige datatyper: • Personoplysninger, fortrolige/følsomme • Personoplysninger, almindelige • Værdioplysninger • Interne data • Åbne data	**A.8.2 Klassifikation af information** Målsætning: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen. **Kontrolspørgsmål:** Er information klassificeret efter lovmæssige krav, værdi og efter, hvor følsom og kritisk informationen er i forhold til uautoriseret offentliggørelse eller ændring?	Ingen bemærkninger	

Organisationsområde i Københavns Kommune	KIT	Område/emne	Kontroller relateret til cybersecurity

Ref.	Observation	Kontrolområde og kontrolspørgsmål/ risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed
Gennemgang af kontroller relateret til cybersecurity				
A.15 Leverandørforhold	Vi har fået oplyst, at der foretages overvågning af leverandørydelser på flere niveauer. Der indhentes årlige revisionserklæringer som en del af den kontrol, som Københavns Kommune selv gennemfører. Derudover har systemejere ansvaret for løbende at kontrollere de leverede ydelser. Ydermere er Contract Management pålagt ansvaret for en kontinuerlig opfølgning af service level agreements. Endvidere har vi observeret, baseret på Københavns Kommunes egen erfaring, at proceduren for tildeling af adgange til eksterne konsulenter ikke følges konsekvent, og at der ikke laves løbende opfølgning på de eksterne konsulenters handlinger på det administrative netværk. Vi har dog fået oplyst, at implementeringen af et system til monitorering af eksterne konsulenters handlinger er startet i november 2015. Endelig er det konstateret, at der grundet manglende central styring af leverandøradgange ofte anvendes fællesbrugere af de af leverandørens medarbejdere, der tilgår kommunens systemer. Området er af Københavns Kommune identificeret som særligt fokusområde. Vi har fået oplyst, at KIT efter beslutning i Borgerrepræsentationen den 30. april 2015 har gennemført et omfattende analysearbejde, der har ført til forslag om anskaffelse af en samlet IDM-løsning, der muliggør både samlet styring af eksterne leverandørers adgange og løbende ledelsesmæssig opfølgning på disse. **Status november 2016** Vi har fået oplyst, at der i forbindelse med implementeringen af SIEM-løsningen vil være en logning af eksterne leverandørers adgange samt opfølgning herpå. Endvidere er det oplyst, at der er etableret konkrete retningslinjer for tildeling og styring af leverandøradgange, men at processen endnu ikke sikrer, at der gennemføres en løbende ledelsesmæssig opfølgning på, hvorvidt leverandørerne overholder de sikkerhedskrav, som er stillet af Københavns Kommune.	**A.15.2 Styring af leverandørydelser** Målsætning: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne. **Kontrolspørgsmål:** Overvåges, auditeres og gennemgås leverandørydelserne løbende?	Vi henstiller til, at der etableres konkrete retningslinjer for tildeling, styring og opfølgning på leverandøradgange, samt at denne proces forankres på et så tilstrækkeligt niveau, at der kan gennemføres en løbende ledelsesmæssig opfølgning.	

Organisationsområde i Københavns Kommune	KIT	Område/emne	Kontroller relateret til cybersecurity

Ref.	Observation	Kontrolområde og kontrolspørgsmål/ risikobeskrivelse	Anbefaling/vurdering	Risiko og Væsentlighed
Gennemgang af kontroller relateret til cybersecurity				
A.18 Overensstemmelse	Der er udarbejdet flere politikker, der beskriver beskyttelse af privatliv og personoplysninger: • it-sikkerhedspolitik • it-sikkerhedsregulativ • Uddybende it-sikkerhedsregler, herunder sikkerhedshåndbog. Det er oplyst, at it-sikkerhedsregulativet og de uddybende it-sikkerhedsregler tager udgangspunkt i ISO 27001-2, og at it-sikkerhedsniveauet lever op til lovgivningens krav, herunder kravene i persondataloven. Derudover har vi fået oplyst, at tildeling af adgange til personfølsomme data skal godkendes af autorisationsansvarlige. Der er udarbejdet vejledninger til, hvorledes personfølsomme data skal behandles. Ydermere foretages som noget nyt en systematisk scanning af Københavns Kommunes websites med henblik på at gennemgå filer, der kunne være tilgængelige for alle, og som indeholder personfølsomme data.	**A.18 Overensstemmelse med lov- og kontraktkrav** Målsætning: At forhindre overtrædelse af lov-, myndigheds- eller kontaktkrav i relation til informationssikkerhed og andre sikkerhedskrav. **Kontrolspørgsmål:** Er privatliv og personoplysninger beskyttet?	Ingen bemærkninger	

Forvaltningens iværksatte tiltag	
	Vi har ikke foretaget revision af de af forvaltningen beskrevne tiltag, jf. nedenstående, men vil følge op herpå i forbindelse med revision af 2017.
	2015 -A15.2. Styring af leverandørydelser. KS er enig i, at styringen på området hidtil ikke har været tilstrækkelig. Risikoen er identificeret i KS' baselinerisikovurdering pr. 30.6.2015, og KS har i september 2015 anskaffet et produkt, som vil muliggøre en standardiseret og logbar adgang for eksterne leverandører. Der etableres kontrol- og logningsspor i forbindelse med etablering af central logningsløsning (SIEM). Dermed vil KS kunne sikre en forbedret styring af leverandøradgange fra primo 2016. KS har efter beslutning i Borgerrepræsentationen den 30. april 2015 gennemført et omfattende analysearbejde, der har ført til forslag om anskaffelse af en samlet IDM-løsning, der muliggør både samlet styring af eksterne leverandørers adgange og løbende ledelsesmæssig opfølgning på disse. Forslaget rummer andre store sikkerhedsmæssige forbedringer og vil blive fremlagt til politisk behandling i løbet af kort tid. Såfremt det besluttes at bevilge de nødvendige midler til etablering af den foreslåede IDM-løsning, vil det være muligt at etablere en samlet, løbende opfølgning på leverandøradgange fra primo 2017. **2016 – A.15** KIT arbejder målrettet hen imod, at SIEM muliggør en standardiseret og logbar registrering af eksterne leverandører, således at der kan etableres kontrol- og logningsspor i forbindelse med eksterne leverandøradgange. En sådan løsning er etableret for den centrale brugerstyring (AD) samt for nogle lokale fagsystemer, som der aktuelt arbejdes med. BR har forbindelse med Budget 2017 på forslag af ØKF vedtaget, at KK anskaffer IDM-løsning, som muliggør både samlet styring af eksterne leverandørers adgange og løbende ledelsesmæssig opfølgning på disse. Intern revision deltager som observatør i anskaffelsesprojektets styregruppe. Det påregnes, at første ledelsestilsyn på området vil kunne finde sted ultimo 2017 eller i maj 2018, afhængig af den valgte udbudsform.

4. Formidling af risiko og væsentlighed mv.

Vi har vurderet graden af risiko og væsentlighed for de enkelte observationer. Risiko og væsentlighed er målrettet den reviderede decentrale enhed, hvor fejl kun ekstraordinært vil kunne give en fejl i det samlede regnskab. I tilknytning til den givne observation har vi påført en prioritet ud fra følgende vurderingsgrundlag:

Prioritet 1 – markeres med 

- Prioritet 1-markeringer anvendes for risici, der anses for kritiske. I forbindelse med beretninger kan det observerede forhold efter nærmere vurdering eventuelt give anledning til en revisionsbemærkning.
- En risiko 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.
- Observationen medtages i delberetninger og beretninger til Borgerrepræsentationen.

Prioritet 2 – markeres med 

- Prioritet 2-markeringer anvendes for risici, der anses for væsentlige. Observationerne må ikke have en karakter, der kan medføre revisionsbemærkninger i årsberetningen.
- En risiko 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.
- Observationen medtages ikke i delberetninger og beretninger.

Prioritet 3 – markeres med 

- Anvendes for risici, der 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.

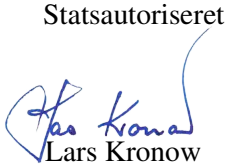
5. Afslutning

Nærværende rapport har i udkast været drøftet med relevante personer for afklaring af eventuelle faktuelle fejl.

Vi står naturligvis til disposition, såfremt De måtte have spørgsmål eller kommentarer til rapporten.

København, den 23. maj 2017

Deloitte
Statsautoriseret Revisionspartnerselskab



Lars Kronow
statsautoriseret revisor

Lars Holm Sørensen
partner, CISA

c.c.: Intern Revision