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
Att.: Mikkel Hemmingsen
Rådhuspladsen 1
1550 København V

It-sikkerhedsarbejdet på udvalgte områder i Københavns Kommune

Revisionsrapport

Indledning

Deloitte har i overensstemmelse med revisionsudvalgets beslutning den 7. april 2015 og som led i forvaltningsrevisionen foretaget et supplerende revision af it-sikkerhedsarbejdet i Københavns Kommune baseret på følgende:

- Overordnet interview og gennemgang af enkelte udvalgte kontroller inden for cybersikkerhed
- Overordnet interview og gennemgang af enkelte udvalgte kontroller inden for persondataloven (data privacy) samt
- Indhentet status på det igangværende it-risikostyringsprojekt som er igangsat på baggrund af den udarbejdede ISO 27001 modenhedsanalyse gennemført af PwC

Efterfølgende er undersøgelsen efter aftale med kommunens interne revision blevet udvidet med organisatoriske forhold omkring it-sikkerhed og konstaterede it-sikkerhedshændelser (afsnit 4):

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 adressere væsentlige it-risici på overordnet niveau, som relaterer sig til andre områder end regnskabsaflæggelsen, herunder 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 intern revision og med udgangspunkt i ISO27001, Persondataloven samt det igangværende it-risikostyringsprojekt 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.

Vi har endvidere fået en opdateret status på det igangværende it-risikostyringsprojekt og foretaget en overordnet vurdering af offentligt tilgængeligt materiale særligt borgerrådgiverens rapport om sikring af borgerens personoplysninger, handlingsplaner, budgetindstilling til Borgerrepræsentationen af 10. april 2015 og øvrige tiltag, der er udarbejdet og igangsat.

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

Gennemgangen af udvalgte kontroller samt opfølgning på risikovurderingsprojektet er gennemført som forvaltningsrevision og er i høj grad baseret på interviews og gennemgang af modtaget materiale.

2. Ledelsesresume og konklusion

2.1 Persondataloven

På baggrund af vores gennemgang er det vores vurdering, at der i al væsentlighed er designet retningslinjer for sikring af persondata, herunder at data er klassificeret. Vi har ikke haft mulighed for at verificere, om disse er implementeret i de enkelte forvaltninger men henviser til Borgerrådgiverens udarbejdede rapporter herom.

Ifølge Borgerrådgiverens undersøgelser og rapport angående "Sikring af Borgernes personoplysninger" er det dog konklusionen, at Koncern Service ikke forholder sig aktivt til, hvorvidt forvaltningernes iværksatte tiltag på området er tilstrækkelige, og at der er risiko for, at borgernes personfølsomme oplysninger ikke er sikret imod uberettiget videregivelse, og at medarbejdere uberettiget kan skaffe sig adgang til disse oplysninger. Vi konstaterer, at Koncern Service, i september 2015, har iværksat en handlingsplan, der skal sikre, at Borgerrådgiverens anbefalinger gennemføres.

2.2 Cybersikkerhed

Det er vores opfattelse, at arbejdet med implementering af en fælles risikostyringsmodel fortsat er i fokus og i fremdrift. It-sikkerhedsfunktionen har delt risikostyringsprojektet op i tre faser, hvor første fase med en overordnet vurdering af it-sikkerheden i kommunens infrastruktur er gennemført, og en baselinevurderingsrapport til Koncern Service er udarbejdet. Vi har dog ved vores gennemgang fået udleveret en status og tidsplan for det videre arbejde med projektet og baseret på den i tidsplanen anførte status, herunder at projektet allerede er forsinket, skal vi anbefale, at der løbende allokeres ressourcer i både Koncern Service og forvaltningerne til at udføre de aktiviteter, planen foreskriver for at sikre projektets fremdrift og overholdelse af angivne deadlines.

Baseret på det materiale, der har været tilgængeligt omkring risikostyringsprojektet, er det vores vurdering, at fokus på teknik og systemer overskygger fokus på it-sikkerhedsledelsesaspektet, idet det ikke fremgår tydeligt, hvorvidt der er afsat midler og ressourcer til eksempelvis overvejelser om placering af roller, ansvar samt beslutninger om, hvor ansvaret skal placeres for de enkelte sikkerhedsområder og de styringsmæssige aspekter.

Vi har fået oplyst, at der ikke sker nogen systematisk opfølgning på om medarbejdere i modstrid med reglerne opbevarer persondata på bærbare computere, og vi har konstateret, at retningslinjer for styring af mobile enheder (telefoner og tablets) først nu er under implementering. Vi anbefaler, at der fastlægges og implementeres retningslinjer for håndtering af persondata på bærbare enheder, herunder både computere og telefoner, og at det sikres, at alle data er hensigtsmæssigt beskyttet.

Der er indgået kontrakt med eksterne leverandører, som løbende holder øje med netværkstrafikken. Vi anbefaler, at der sker en forankring af opfølgningen på monitorering i it-sikkerhedsafdelingen, således at dette kan indgå i den generelle it-sikkerhedsmæssige opfølgning, herunder at der foretages opfølgning på brud på it-sikkerheden. Vi har fået oplyst, at it-sikkerhedsafdelingen først pr. september 2015 har etableret opfølgning på hændelser mv., idet processerne med overvågning indtil da har ligget uden for it-sikkerhedsafdelingen. Vi har fået oplyst, at Københavns Kommune pt. er i gang med at implementere et log-overvågningssystem på netværket.

2.3 ISO 27001 modenhedsanalyse

Vi har observeret, 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. 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 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.

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 effektivt implementeres i organisationen. I den kommende persondatalovsforordning stilles der krav om, at der udpeges en databeskyttelsesansvarlig, som er uafhængig og rapporterer direkte til ledelsen hos dataejer (ansvarlige). Vigtigheden af korrekt placering af roller og ansvar for it-sikkerhedsarbejdet i kommunen understreges heraf. Vi stiller os derfor tvivlende ved, at de igangsatte tiltag er tilstrækkelige til at opnå det ønskede modenhedsniveau, da hovedfokus synes at foreligge på værktøjer og systemer. Det ønskede modenhedsniveau er 4 på en skala på 1 – 5, hvor det nuværende modenhedsniveau vurderes at være 1,8.

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.

Efter det oplyste skal der for begge områder udføres en yderligere og mere detaljeret risikovurdering, som skal følges op med yderligere tiltag for at højne sikkerheden på områderne. Dette understøttes ligeledes af borgerrådgiverens rapport om sikring af borgernes personoplysninger. Vi anbefaler, at arbejdet med udbedring af de fundne svagheder prioriteres, og at det sikres, at der allokeres tilstrækkelige ledelsesmæssige ressourcer hertil, samt at der løbende følges op herpå.

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 2016.
	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 Koncernservice vil levere yderligere complianceredskaber og udbygget, konkret rådgivning til forvaltningerne. Handlingsplanen vil indeholde forslag om at It-sikkerhedsfunktionen i Koncernservice 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.

3. Observationer, risikovurdering og anbefaling

3.1 Oversigt over observationer

Vi har 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 KK	Koncernservice	**Område/ emne**	Kontroller relateret til Persondataloven

Ref.	**Observation**	**Kontrolområde og kontrolspørgsmål / risikobeskrivelse**	**Anbefaling / vurdering**	**Risiko & 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 udføreres for at skabe et samlet risikobillede. Vi har fået oplyst, at risici i forhold til kritiske aktiver i netværket, hvor Koncern Service 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.	**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 både i Koncern Service og i forvaltningerne løbende allokeres tilstrækkelige ressourcer til projektet såvel ledelsesmæssigt som udførende for at sikre den videre frem-drift.	
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-sikkerheds-afdelingen 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.	

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. Vi har dog fået oplyst, at der ikke er planlagt fremtidige kampagner på nuværende tidspunkt.	
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 2016.			
	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 er 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.			

Organisationsområde i KK	Koncernservice	Område/ emne	Kontroller relateret til Cyber Security

Ref.	Observation	Kontrolområde og kontrolspørgsmål / risikobeskrivelse	Anbefaling / vurdering	Risiko & Væsentlighed
Gennemgang af kontroller relateret til Cyber Security				
1. Risikovurdering	Vi har fået oplyst, at Københavns Kommune i samarbejde med PwC har foretaget en modenhedsanalyse, som har resulteret i en risikostyrings-model, der beskriver de aktiviteter, som skal udføreres for at skabe et samlet risikobillede. Vi har endvidere fået oplyst, at risici i forhold til kritiske aktiver i netværket, hvor Koncern Service har ansvaret, er identificeret, og at næste step er at identificere risici i forhold til de enkelte forvaltninger. Projektet forventes afsluttet ultimo 2015.	**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 både i Koncern Service og 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 Koncern Service har etableret et samlet It-beredskab, der også håndterer hændelser i forhold til Cyber Security, 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.	
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".	**Data sikkerhed:** Målsætning At sikre datasikkerhed for data i transit? **Kontrolspørgsmål:** Er data i transit beskyttet?	Vi henstiller til, at der etableres 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 sikkerheds-hændelser, 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 KK	Koncernservice	Område/ emne	Kontroller relateret til Cyber Security

Ref.	Observation	Kontrolområde og kontrolspørgsmål / risikobeskrivelse	Anbefaling / vurdering	Risiko & Væsentlighed
Gennemgang af kontroller relateret til Cyber Security				
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-sikkerheds-afdelingen 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-sikkerheds-hændelser, og at disse løbende afrapporteres til et nyetableret Ledelsesforum for it-sikkerhed i Koncern Service. Derudover har vi fået oplyst, at Københavns Kommune pt. er i gang med at implementere et log-overvågningssystem på netværket.	**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 cyber security?	Vi henstiller til, at Koncern Service sikrer, at de netop i oktober 2015 indførte rutiner fungerer, så der som minimum sker en forankring af opfølgningen på monitorering i it-sikkerhedsafdelingen, således at dette kan indgå i den generelle it-sikkerhedsmæssige opfølgning.	

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 2016.
	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 er 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 har KS tidligere i 2015 anskaffet et produkt, som vil muliggøre kryptering på særligt udvalgte PC efter konkret bestilling. Yderligere vil data på alle bærbare Pc 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. og det er tidligere besluttet, at IT-sikkerhedsfunktionen skal gennemføre en ny awareness-kampagne 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 at forankring af opfølgningen i It-sikkerhedsafdelingen er implementeret i oktober 2015 jf. den beskrevne observation.

Organisationsområde i KK	Koncernservice	Område/ emne	ISO 27001 Kontroller

Ref.	Observation	Kontrolområde og kontrolspørgsmål / risikobeskrivelse	Anbefaling / vurdering	Risiko & 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	
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 Koncern Service efter beslutning i Borgerrepræsentationen 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 dem.	**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.	

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 2016.			
	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 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 dem. 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.			

4. Status på it-risikostyring

Vi har på baggrund af interview med Jens Ingemann og Brian Thordarson foretaget en opfølgning på det igangværende it-risikostyringsprojekt. En ekstern vurdering af kommunens modenhed på it-sikkerhedsområdet har påpeget, at der bør etableres en fælles metode til risikostyring med klar ansvarsfordeling, så der kan leveres omkostningseffektiv informationssikkerhed i en styret proces. Projektet er tilrettelagt med følgende tre hovedfaser:

1. Der skal etableres en overordnet baselinevurdering af it-sikkerheden i kommunens infrastruktur. Infrastrukturen opdeles og vurderes i fem kategorier: Adgangsstyring, netværk og kommunikationslinjer, driftscentre, PC og mobile enheder samt andre enheder (eksempelvis printere mv.).
2. Arbejdet med vurdering af baseline bruges som udgangspunkt for etablering af en risikostyringsproces for de af kommunens fagsystemer, der afvikles på den fælles infrastruktur.
3. Der skal etableres risikostyring af eksterne driftsleverandører.

Målet med de samlede tiltag er at opnå et modenhedsniveau 4 ud af 5 i forhold til nuværende 1.8. Vi har i den forbindelse bemærket, at sikkerhedsprojekterne hovedsageligt indeholder elementer af teknisk karakter som eksempelvis log management løsning, ny netværksinfrastruktur, IDM løsning mv.

Vi har fået oplyst, at It-sikkerhedsfunktionen har påbegyndt anden fase af risikostyringsprojektet, hvor planlægning af risikovurderingsforløb med de respektive forvaltninger er igangsat. I denne fase defineres de mest kritiske systemer af de respektive forvaltninger og risikovurderinger gennemføres i samarbejde med it-sikkerhedsfunktionen. Det bemærkes, at projektet i første omgang er rettet mod de mest kritiske systemer, og når processen er færdig, vil man påbegynde gennemgang af de øvrige systemer. Ydermere har vi fået oplyst, at gennemførelse af risikovurderinger for TMF er påbegyndt.

Det er over for os oplyst, at projektet med identificering af risici samt udarbejdelse af handlingsplaner for såvel risici i relation til it-infrastrukturen samt i de enkelte forvaltninger forventes afsluttet i overensstemmelse med den revurderede tidsplan inden udgangen af 2015. Det bemærkes, at en væsentlig forudsætning for tidsplanens overholdelse vil være, at de enkelte forvaltninger gennemfører en risikovurderingerne rettidigt.

Der er på nuværende tidspunkt identificeret svagheder undervejs i projektet, hvor yderligere tiltag og mere detaljerede risikoanalyser er påkrævet.

5. 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.

6. 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 19. januar 2016

Deloitte
Statsautoriseret Revisionspartnerselskab

Ulrik Vassing
statsautoriseret revisor

Lars Holm Sørensen
partner, CISA

c.c.: Koncernservice og Intern Revision