KØBENHAVNS KOMMUNE
Økonomiforvaltningen
Koncern IT

NOTAT

14-08-2017

Sagsnr.
2017-0285879-3

Dokumentnr.
2017-0285879-3

Sagsbehandler
Jens Ingemann

Til Økonomiudvalget

Orientering om rapporten vedrørende "Undersøgelse og vurdering af gennemført tilsyn med it-sikkerhed 2016"

Sagsfremstilling
Intern Revision har fremsendt intern rapport til Økonomiforvaltningen, og Ekstern Revision Deloitte, vedrørende undersøgelse og vurdering af det tilsyn med it-sikkerhed, som Koncern IT har udført i 2016.

Koncern IT har i 2016 gennemført tilsyn med forvaltningernes efterlevelse af bestemmelserne i it-sikkerhedshåndbogen. Den overordnede tilrettelæggelse af tilsynet er sket i samarbejde mellem Koncern IT, Intern Revision og Ekstern Revision.

Det udførte tilsyn har ikke givet anledning til bemærkninger fra Ekstern Revision i 2016.

Løsning
Rapportens hovedkonklusioner

- Intern Revision vurderer, at den foreliggende dokumentation er egnet i forhold til at konkludere på de foretagne tilsyn, men at tilsynet kun giver en mindre indsigt i kommunens it-sikkerheds- og risikoniveau
- Intern Revision anbefaler, at det i 2017 prioriteres at få etableret en systematisk og risikobaseret tilgang til tilsynet med it-sikkerhed i Københavns Kommune, og der udarbejdes en ramme for de fremtidige tilsyn, som kan implementeres fra den 1. januar 2018.

Videre proces
Økonomiforvaltningen har igangsat arbejdet med at tilrettelægge de fremtidige tilsyn fra 2018 jævnfør Intern Revisions anbefalinger.

Bilag
Bilag 1: Rapport fra Intern Revision vedrørende "Undersøgelse og vurdering af gennemført tilsyn med it-sikkerhed 2016"

KØBENHAVNS KOMMUNE
INTERN REVISION

10. juli 2017

RAPPORT

Rapport vedrørende undersøgelse og vurdering af gennemført tilsyn med it-sikkerhed 2016 2016

MODTAGER

Mads Grønvall
Stig Lundbech
Jens Ingemann

Indholdsfortegnelse

1. INDLEDNING OG FORMÅL 3
2. LEDELSESRESUME 4
3. KONKLUSION 4
4. FORVALTNINGENS TILTAG 8

1. INDLEDNING OG FORMÅL

Intern Revision (IR) har i overensstemmelse med revisionsplanen for 2016 og ledelsesmæssige beslutninger er foretaget en undersøgelse og vurdering af it-sikkerhedsfunktions (ITS) tilsyn med it-sikkerheden i 2016.

ITS's opgaver fremgår af It-sikkerhedsregulativet og tilhørende bestemmelser, og består af tilsyns- og kontrolopgaver samt mere driftsrettede it-sikkerhedsopgaver.

Tilsyn/kontrol er således ikke organisatorisk adskilt fra funktionens mere driftsrettede it-sikkerhedsopgaver samt de øvrige it-drift områder i Koncern IT (KIT), hvilket kan påvirke tilsynets resultater. Derfor er det aftalt, at IR for 2016 foretager en vurdering af ITS's tilsyn, som følge af den manglende organisatoriske funktionsadskillelse.

På baggrund af anbefalinger og bemærkninger fra Ekstern Revision og Borgerrådgiveren, er der udvalgt følgende tilsynsområder i 2016:

- Uddannelse og rådgivning
- Compliance i forhold til sikkerhedsbestemmelser
- Adgangsrettigheder og adfærd
- Risikovurdering

Den overordnende tilrettelæggelse af tilsynet er sket i samarbejde mellem Koncern IT, Intern Revision og Ekstern Revision.

Nærværende undersøgelse er fastlagt ud fra en vurdering af væsentlighed og risikoen for væsentlige fejl i relation til **Compliance,** der betyder, at kommunen ikke disponerer i overensstemmelse med gældende lovgivning, politiske beslutninger, meddelte bevillinger og øvrige beslutninger eller i overensstemmelse med indgåede aftaler og sædvanlig praksis. I relation til it-sikkerhed kan manglende compliance betyde øget risiko for sikkerhedshændelser.

Rapporten forelægges ØKF/KIT og Ekstern Revision.

Formålet med undersøgelsen, er at bedømme:

Tilsynets tilrettelæggelse og gennemførelse herunder:

- Dækker tilsynet de områder, som ITS har ansvaret for, og som er beskrevet i it-sikkerhedsregulativ og tilhørende bestemmelser.
- Er der eventuelt sammenfald mellem medarbejdere, der har gennemført tilsynet, og medarbejder der har udført sikkerhedsarbejdet.
- Er tilsynet i øvrigt gennemført, så det giver et retvisende billede af de områder, der er undersøgt.

Tilsynets observationer

- Giver de forhold, der er observeret som følge af tilsynet, anledning til væsentlige konklusioner.

2. LEDELSESRESUME

Intern Revision (IR) har gennemført en undersøgelse af it-sikkerhedsfunktions (ITS) tilsyn med it-sikkerheden i 2016. Formålet er at vurdere tilrettelæggelsen, gennemførelsen samt observerede forhold.

Tilsynet har omfattet elementer inden for de aftalte områder, og i al væsentlighed er det vores vurdering, at den foreliggende dokumentation er egnet i forhold til at konkludere på de foretagne tilsyn.

Med det gennemførte tilsyn opnår ITS dog kun en mindre indsigt i kommunens it-sikkerheds- og risikoniveau. Som konsekvens heraf kan kommunen på meget væsentlige it-områder være uvidende om omfanget af interne sårbarheder og eksterne trusler.

Det er IR's vurdering, at ITS i 2017 bør fokusere på at opnå en systematisk og risikobaseret tilgang til tilsynet med it-sikkerhed i Københavns Kommune.
Det er således vores anbefaling, at det i 2017 prioriteres at få udarbejdet en ramme for de fremtidige tilsyn, som kan implementeres fra 1. januar 2018.

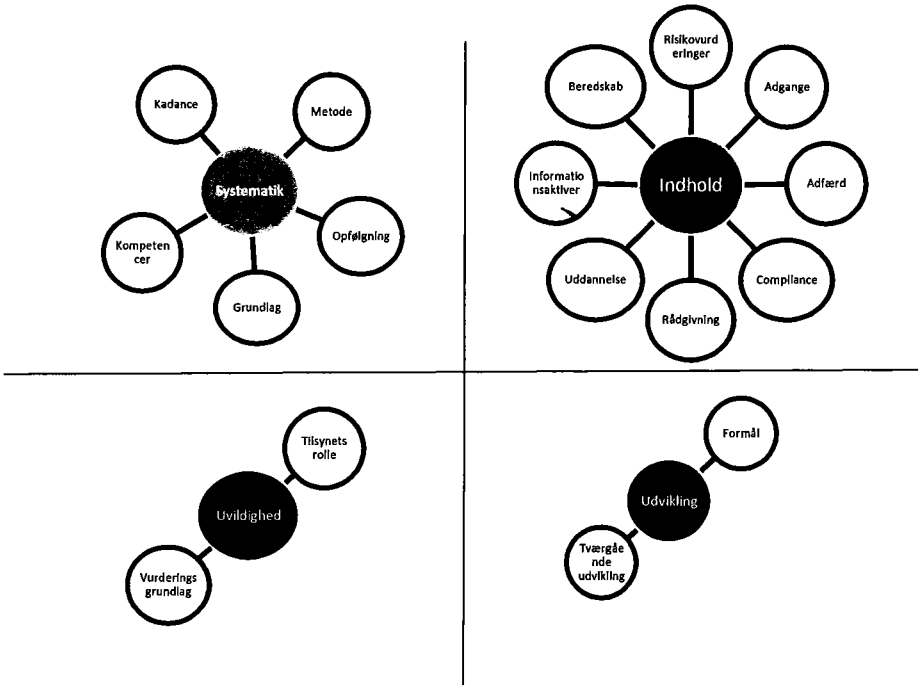
ITS har ansvaret for den tværgående koordinering af beredskabsplaner. Derfor er det særligt kritisk, at tilsynet konkluderer, at kommunens forvaltninger ikke samarbejder med ITS om at tilrettelægge disse beredskabsplaner. Konsekvensen er, at it-understøttede forretningsprocesser i tilfælde af større nedbrud kun kan genetableres ved anvendelse af væsentlige økonomiske og menneskelige ressourcer samt tid.

Der henvises i øvrigt til afsnit 3 hvor en række yderligere observationer fremgår.

3. KONKLUSION

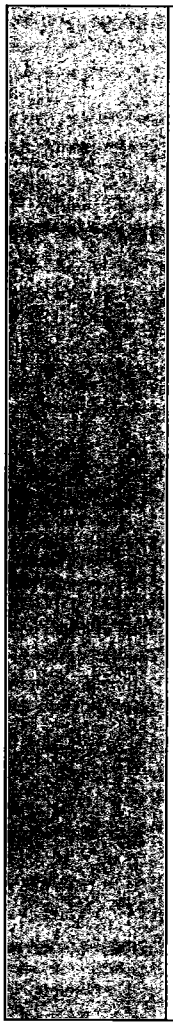
På grundlag af vores gennemgang af it-sikkerhedsfunktions (ITS) tilsyn med it-sikkerheden i 2016, kan vi drage følgende konklusioner:

Forvaltning	ØKF / KIT	**Revisionsområde**	Tilsyn med IT-sikkerhed
Reference	3.1	**Revisionsemne**	Tilsynets tilrettelæggelse og gennemførelse
Observationer	Den overordnende tilrettelæggelse af tilsynet er sket i samarbejde mellem Koncern IT, Intern Revision og Ekstern Revision og retter sig mod følgende områder: • Uddannelse og rådgivning • Compliance i forhold til sikkerhedsbestemmelser • Adgangsrettigheder og adfærd • Risikovurdering Tilsynet har omfattet elementer inden for de aftalte områder og i al væsentlighed er det vores vurdering at den foreliggende dokumentation er egnet i forhold til at konkludere på de foretagne tilsyn.		

	Tilsynet dækker dog kun en mindre del af områder, som ITS har ansvaret for, og som er beskrevet i it-sikkerhedsregulativ og tilhørende bestemmelser. Herunder skal bemærkes, at en vis del af det gennemførte tilsyn ikke vurderer sikkerhedsniveauet, men giver en status på igangværende projekter, som på sigt skal understøtte kommende it-sikkerhedstilsyn. Der er ikke i alle tilfælde funktionsadskillelse, mellem udførende medarbejderen og tilsynsmedarbejder. ITS synes usikker i forhold til at planlægge, gennemføre og formidle tilsynet. Blandt andet er der visse observationer, der burde være yderligere undersøgt ligesom rapportering ikke er helt tydelig.
Anbefaling	Det anbefales, at der etableres en ramme for udførelse af tilsynet med IT-sikkerheden i Københavns Kommune. Rammen for dette arbejde kan med fordel bestå af fire centrale temaer: • *Systematik, indhold, uvildighed og udvikling* Hvert tema består af en række delelementer. Systematik er generelle forhold som bør iagttages i forbindelse med udførelse af tilsyn. Temaerne indhold, uvildighed og udvikling er identificeret i kommunens sikkerhedsregulativ.  **Systematik** handler om, at man skal sikre, at alle områder får et ensartet tilsyn, at man kommer omkring alle de elementer, som der skal føres tilsyn med, at der er et tydeligt grundlag at føre tilsyn ud fra, og at man husker at følge op på tilsynet. Endelig er det vigtigt, at man har kendskab til de metoder, der med fordel kan anvendes i de konkrete situationer, og at medarbejderne har de nødvendige kompetencer og metodekendskab. Et systematisk grundlag handler om at nedskrevne kriterier, kvalitative beskrivelser eller et særligt koncept/redskab til at vurdere det man ser. **Indhold** handler om, at tilsynet skal sikre, at it-sikkerhedsarbejdet lever op til de krav som stilles. Tilsynet skal indeholde de obligatoriske elementer, der fremgår af stilles i it-sikkerhedsregulativet, sikkerhedsbekendtgørelsen m.v. **Uvildighed** handler om den rolle som tilsynet i øvrigt har over for institutionerne og om tilsynet føres på et tydeligt grundlag eller ud fra den tilsynsførendes individuelle skøn. Et uvildigt tilsyn bør baseres på et klart vurderingsgrundlag, eks. i form af kriterier, kvalitative beskrivelser af god praksis eller et koncept/redskab.

	Udvikling handler, om hvorvidt tilsynet kan bidrage til at skabe udvikling, og hvordan viden anvendes til at udvikle it-sikkerheden på tværs af forvaltningerne. Der bør være et udviklingsperspektiv i tilsynet, så tilsynet ikke bare er kontrol. Det er således vores anbefaling at det i 2017 prioriteres at få udarbejdet en ramme for de fremtidige tilsyn som kan implementeres fra 1. januar 2018.		
Forvaltningens iværksatte tiltag			
Forvaltning	ØKF / KIT	**Revisionsområde**	Tilsyn med IT-sikkerhed
Reference	3.2	**Revisionsemne**	Tilsynets observationer
Observationer	Det af ITS udførte tilsyn har givet anledning til følgende observationer: **Uddannelse og rådgivning** Implementeringen af awareness kampagnen er afsluttet fra ITS's side på det tidspunkt, hvor formidlingen til forvaltningen er foretaget. Der er ikke foretaget en opfølgning på, om kampagnen er nået ud til modtagerne. Awareness kampagnen har ikke omfattet en sikring af at kampagnen har haft en effekt. På grundlag af få forespørgsler til forvaltningerne viser tilsynet dog, at medarbejderne i forvaltningerne er informeret om kampagnen. **Compliance i forhold til sikkerhedsbestemmelser** *Sundhedstjek* - ITS har etableret et sundhedstjek, der skal føre til fortegnelse af kommunens informationsaktiver herunder tilhørende information og dokumentation. Projektet er i sin indledende fase, hvorfor tilsynet kun berører den mindre del af kommunens systemportefølje, hvor sundhedstjek er gennemført. Informationer / dokumentation som følge af sundhedstjekket er i visse tilfælde ikke retvisende. ITS varetager endvidere registrering af hardware og tekniske aktiver i CMDB system. Det kan konstateres, at KIT ikke har et tilstrækkelig overblik / dokumentation for disse aktiver på nuværende tidspunkt. *Håndtering af it-sikkerhedshændelser* sker på grundlag af en delvist dokumenteret proces. Der er dog et utilstrækkelig samarbejde med forvaltningerne herunder ved dokumentation af indmeldinger. Der er derfor ikke sikkerhed for, at alle hændelser indmeldes til ITS, og at der dermed er iværksat handlinger for at imødegå disse. Manglede indmeldinger kan også underminere den fastsatte ledelsesrapportering jf. IT-sikkerhedsregulativet og den eventuelle indrapportering til Datatilsynet. *Beredskabsstyring* foretages af ITS for KS og KIT. På trods af, at ITS har ansvaret for, at der foreligger procedurer, der sikrer tværorganisatoriske styring af it beredskab i tilfælde af større nedbrud, har det ikke været muligt for ITS at tilrettelægge beredskabsplaner for it-understøttede forretningsprocesser i forvaltningerne. På undersøgelsestidspunktet har forvaltningerne ikke besvaret ITS's henvendelser. De manglende procedurer udgør væsentlig risiko for kommunen. *Håndtering af anmodning af indsigt* fra borger er grundliggende i orden. Dog foreligger der ikke en dokumenteret proces, der sikrer, at korrekte systemer omfattes undersøgelsen, når borgere skal oplyses, hvilke behandling af personoplysninger, der har fundet sted. Ligeså er det alene systembehandlinger der undersøges, på trods af at der kan foregå behandlingsaktiviteter i andre sammenhænge.		

	Håndteringen af udtjente PC-er sker ikke på grundlag af en end-to-end proces og en forretningsgang. Uden et samlet procesoverblik kan eventuelle uhensigtsmæssige/ risikobetonede områder ikke identificeres i tilstrækkelig grad og dermed hvor kompenserende kontroller er nødvendige. Tilsynet har vist konkrete områder, hvor processen kan være særlig risikofyldt, men hvor der ikke er etableret kompenserende kontroller. **Adgangsrettigheder og adfærd** På de udvalgte områder (KØR og AD) viser ITS's tilsynet, at der foretages ledelsestilsyn i forvaltningerne i henhold til forretningsgange. ITS tilsynet behandler ikke givne resultater af den kontrol, der er foretaget af ledelsen. SIEM løsningen, der skal være grundlaget for en automatiseret logopfølgning, er i den første del af implementeringen, og er frivillig for forvaltninger at anvende. IDM løsningen, der skal sikre korrekt oprettelse, ændringer og nedlæggelse af brugere og adgange, er ikke implementeret endnu. **Risikovurdering** Status er, at der er udarbejdet proces for en baseline risikovurdering af kommunens infrastruktur, herunder en kort beskrivelse af historik og ønskede kommende handlinger. Risikovurdering af systemer er i planlægsfasen, og der er afsat ressourcer hertil, men der er ikke udarbejdet risikoproces, procedurer, værktøjer mv. med udgangen af 2016.
Anbefaling	En del af de observationer som er fremkommet ved tilsynet, er allerede en del af det sikkerhedsprogram som KIT har udarbejdet i marts 2017. Det henstilles, at der følges op på tilsynets observationer og at det sikres, at it-sikkerhedsopgaver i øvrigt løses, som de er foreskrevet i It-sikkerhedsregulativet, således at it-sikkerheden er optimal, frem til at understøttende sikkerhedssystemer og processer er implementeret. KIT's ledelse bør i samme forbindelse tager stilling til, hvordan observationerne skal anvendes i et udviklingsperspektiv. IR finder det særligt kritisk, at kommunens forvaltninger ikke samarbejder med ITS om at tilrettelægge beredskabsplaner. Konsekvensen er, at it-understøttede forretningsprocesser i tilfælde af større nedbrud kun kan genetableres ved anvendelse af væsentlige økonomiske og menneskelige ressourcer samt tid.
Forvaltningens vurdering af tiltag	**Sundhedstjek** Da denne opgave har et formål, der ligger meget tæt op ad Legal Compliance Programmet løftes gennemgangen af systemer fremover over i LCP. LCP-projektet vil sikre, at systemer med fortrolige/følsomme personoplysninger bliver gennemgået og systemdokumentation opdateret, og opfølgning vil blive indarbejdet i de løbende driftsopgaver efter afslutning af LCP-projektet. CMDB og Fiskk er nu integreret i Kommunens nye ITSM system Service Now, og der er dermed skabt sammenhænge/overblik mellem incident (hændelse) registrering/behandling og tilhørende Aktiv (CI). **Håndtering af it-sikkerhedshændelser** ITS har udarbejdet intern to-be proces for behandling af It-sikkerhedshændelser med henblik på implementering i Service Nows "Incident modul". Det forventes at løsningen kan ibrugtages i Q3 2017. Det er aftalt med DCK at der etableres proces og værktøjer, der sikrer, at alle sikkerhedsincidents registreres af IT-sikkerhedsfunktionen i KIT, og at der sker struktureret opfølgning i samarbejde med forvaltningerne. Resultaterne skal indgå i arbejdet med risikostyring i forvaltningerne. Der er etableret et særligt

	projekt i Sikkerhedsprogrammet, som skal sikre at udformning og implementering af proces skal ske i samarbejde mellem forvaltningerne og KIT På denne måde etableres der et entydig indberetnings- og behandlingsspor. **Beredskabsstyring** KIT har udarbejdet et paradigme for specialplan for beredskab for it-understøttede processer i forvaltningerne jf. tilsynsrapporten vedr. forankring af at opfølgning i IT-sikkerhedsafdelingen. BSKK besluttede på sit møde den 26-11-2014 at den enkelte forvaltning selv, enten i forvaltningernes egne Delplaner for "Plan for Fortsat drift" eller i en Specialplan (udarbejdet efter KS paradigme) skal beskrive de foranstaltninger og tiltag, der skal iværksættes i tilfælde af problemer med forretningskritiske IT systemer. ITS har i overensstemmelse med tilsynets anbefaling rejst spørgsmålet om forvaltningernes implementering af it beredskab ved BSKK. BSKK har på sit seneste møde drøftet spørgsmålet og besluttet at de enkelte forvaltninger aktivt skal overveje implementering af ITS anbefalinger. Det er forudsætning for et effektivt samlet beredskab, at forvaltningerne efterlever opfordringen fra BSKK-mødet. ITS vil indenfor disse rammer fortsat følge op og have fokus på forvaltningernes implementering af ITS anbefalinger. **Håndtering af anmodning af indsigt** KIT vil undersøge i hvilket omfang, det kan sikres, at alle relevante systemer indgår i processen for indsigt efter Persondatalovens § 3 – og efter maj 2018 efter databeskyttelsesforordningen. KK (ITS) har ikke hidtil haft kendskab til i hvilket omfang, der foregår behandlingsaktiviteter i andre sammenhænge end i IT-systemer. Det forventes, at LCP (IR) dataflowsanalyser vil belyse i hvilket omfang data fra disse analyser kan danne grundlag for udvælgelse af behandlingsaktiviteter, som borgeren skal underrettes om. **Risikovurdering** ITS har i 2017overtaget ansvaret for risikovurderingsprocessen i forvaltningerne og efter beslutning i BR etableret et risikostyringsteam, som skal sikre, at forvaltningerne får risikovurderet de kritiske systemer, Der er udarbejdet en proces for baseline risikovurdering og etableret årshjul for vurderingen. Pt. er der gennemført en betatest af dels proces og dels værktøj sammen med BIF. Betatesten er baggrund for de kommende risikovurderinger i de øvrige forvaltninger. Gennemførelse af risikovurderingerne planlægges i samarbejde med forvaltningerne, og der afrapporteres til ØU Q1 2018.

4. FORVALTNINGENS TILTAG

Rapports konklusion er drøftet med ledelsen i KIT, der er enig i indholdet af rapporten, og har tilsluttet sig IR risikovurderinger i tilknytning hertil. På dette grundlag har forvaltningen formuleret en række tiltag, som det fremgår ovenfor i afsnit 3.

Forvaltningens ansvarlige for implementering er KIT, IT-sikkerhedsfunktionen
Tidsfrist for afslutning af implementering er jf. ovenfor.

Rapportering

Rapporten forelægges for Revisionsudvalget.