Deloitte

Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
2300 København S

Telefon: 36102030
www.deloitte.dk

IT-Forsyningen I/S
ISAE 3402-erklæring om generelle it-kontroller, Type 2

Erklæringen omfatter perioden 1. januar 2021 til 31. december 2021

Indholdsfortegnelse

1. Serviceleverandørs uafhængige revisors erklæring med sikkerhed

Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til: IT-Forsyningen I/S

Omfang

Vi har fået til opgave at afgive erklæring om IT-Forsyningens beskrivelse i afsnit 3, System- og kontrolbeskrivelse, af driftsydelser og håndtering af de generelle it-kontroller i hele perioden 1. januar 2021 - 31. december 2021 (beskrivelsen) og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

IT-Forsyningen anvender serviceunderleverandørerne Global Connect og TDC til WAN og MPLS. Serviceleverandørens systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandørerne. Denne erklæring er udarbejdet efter partielmetoden og omfatter således ikke kontroller hos serviceunderleverandørerne.

Oplysningerne i afsnit 5, Supplerende information fra IT-Forsyningen, er udarbejdet af IT-Forsyningen for at give yderligere information og skal ikke ses som en del af systembeskrivelsen. Oplysningerne i afsnit 5 er ikke omfattet af vores handlinger, ligesom vores konklusion ikke omfatter oplysningerne i afsnit 5.

Nogle af de kontrolmål, der er anført i IT-Forsyningens beskrivelse af sit system, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos IT-Forsyningen. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementerende kontroller.

IT-Forsyningens ansvar

IT-Forsyningen er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 2, "Serviceleverandørs udtalelse", herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

Deloitte anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om IT-Forsyningens beskrivelse samt om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, *Erklæringer med sikkerhed om kontroller hos en serviceleverandør*, som er udstedt af IAASB. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 2, "Serviceleverandørs udtalelse".

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør

IT-Forsyningens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtige efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i afsnit 2. Det er vores opfattelse,

(a) at beskrivelsen af IT-Forsyningens driftsydelser og de generelle it-kontroller, således som det var udformet og implementeret i hele perioden 1. januar 2021 - 31. december 2021, i alle væsentlige henseender er retvisende

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. januar 2021 - 31. december 2021, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 1. januar 2021 - 31. december 2021.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår af afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt IT-Forsyningens ejerkommuner og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlig fejlinformation i deres regnskaber.

København, den 4. marts 2022

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
partner, statsautoriseret revisor

2. Serviceleverandørs udtalelse

IT-Forsyningens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt IT-Forsyningens driftsydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risicieene for væsentlig fejlinformation i kundernes regnskaber. IT-Forsyningen bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af de driftsydelser, som anvendes af kommunerne i hele perioden 1. januar 2021 - 31. december 2021. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   i. redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

      - de typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, når dette er relevant
      - de processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
      - de tilhørende regnskabsregistreringer, underliggende informationer og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan information blev overført til de rapporter, der er udarbejdet til kunder
      - hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner
      - den proces, der blev anvendt til at udarbejde rapporter til kunder
      - relevante kontrolmål og kontroller udformet til at nå disse mål
      - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomhederne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
      - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner.

   ii. indeholder relevante oplysninger om ændringer i IT-Forsyningens system foretaget i perioden 1. januar 2021 - 31. december 2021.

   iii. ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system, under hensyntagen til at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. januar 2021 - 31. december 2021. Kriterierne for denne udtalelse var, at:

   i. de risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

ii. de identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. januar 2021 - 31. december 2021.

Farum, den 4. marts 2022

IT-Forsyningen I/S

Rasmus Aagaard Winther
direktør

3. System- og kontrolbeskrivelse

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for IT-Forsyningens ejerkommuner og disses revisorer, samt for at opfylde kravene i ISAE 3402-erklæringer med sikkerhed om kontroller hos en serviceleverandør. Beskrivelsen er ligeledes udfærdiget med det formål at give information omkring de kontroller, der anvendes i forhold til levering af IT-Forsyningens services.

Omfang
Beskrivelsen giver oplysninger om de kontroller, der anvendes i forbindelse med implementering, drift og support af de it-services, som leveres af IT-Forsyningen. Beskrivelsen omfatter de it-services, som leveres af IT-Forsyningen, og fokuserer på kontrolmål, der er relevante for de interne kontroller, som relaterer til regnskabsaflæggelsen for IT-Forsyningens ejerkommuner. Beskrivelsen omfatter de væsentligste forretningsprocesser, som IT-Forsyningen har fastslået som væsentlige for deres ejerkommuner ud fra et regnskabsmæssigt synspunkt, tillige med de understøttende, generelle it-kontroller. Ledelsen i IT-Forsyningen er ansvarlig for identifikationen af kontrolmål og for de manuelle og automatiske kontroller, der er sat i drift med henblik på at opnå disse mål. Dette inkluderer den informationsteknologi og infrastruktur, der understøttes af IT-Forsyningens driftsorganisation.

Denne beskrivelse har ikke til formål at omfatte kontrolaspekter i andre dele af IT-Forsyningens organisation, platforme, ydelser eller procedurer for andre af IT-Forsyningens ydelser, som ikke relaterer til it-services leveret til ejerkommunerne. Beskrivelsen er udarbejdet med henblik på generelt at omfatte IT-Forsyningens ejerkommuner. Derfor vil der blive fokuseret på de processer og kontroller, der anvendes i de fælles processer, der understøtter de fælles it-services. Specifikke kundeforhold er ikke inkluderet i denne beskrivelse.

Beskrivelse af IT-Forsyningen
IT-Forsyningen er et selvstændigt interessentskab reguleret af egne vedtægter med en selvstændig økonomi. Selskabets opgave er at levere it-infrastruktur, støtte og en række beslægtede ydelser til ejerkommunerne og samtidig opnå besparelser gennem effektiviseringer i form af kompetenceløft samt harmonisering og konsolidering af de forskellige services, som IT-Forsyningen leverer til ejerkommunerne.

Formålet er, at selskabets service skal understøtte eksisterende og fremtidige krav fra ejerkommunerne og deres borgere, samt at kvaliteten af de leverede services, leveres på et aftalt niveau, og de langsigtede it-omkostninger reduceres.

IT-Forsyningen er ejet af Allerød, Ballerup, Egedal og Furesø kommuner. Allerød indtrådte i ejerskabet pr. 1. september 2018. Rent geografisk dækkes et område på omtrent 284 km², og der serviceres ca. 14.300 it-brugere[1] fordelt på rådhuse, jobcentre, skoler og institutioner, der dækker et samlet befolkningstal på ca. 160.000 indbyggere[2].

IT-Forsyningens vedtægter
Selskabets vedtægter, der er godkendt af Statsforvaltningen, regulerer en række formalia om IT-Forsyningens selskabsfunktion. Vigtigst i denne sammenhæng er §4 og §5, som omfatter henholdsvis selskabets formål samt selskabets pligter og rettigheder.

Interessentskabet har som formål at overtage – herunder samle, effektivisere og videreudvikle – varetagelsen af it-forsyningsopgaven fra ejerkommunerne. Som led i varetagelse af it-forsyning kan selskabet

[1] IT-brugere, der har adgang til IT-Forsyningens Service Desk pr. 24. januar 2021.

[2] Indbyggertal pr. 1. januar 2021 ifølge Økonomi- og Indenrigsministeriets kommunale nøgletal (noegletal.dk)

gennemføre udbud og andre anskaffelser i nødvendigt omfang. Grundlæggende gælder, at ejerkommunerne forpligter sig til ikke at indkøbe ydelser, der er relateret til selskabets formål, af andre end selskabet, jf. pkt. 4 og pkt. 5.2.

Selskabet er forpligtet til at varetage følgende opgaver vedrørende IT-Forsyningen for ejerkommunerne:

- Serverdrift
- Databasedrift
- Datalager (storage)
- Overvågning, backup og styring af it-aktiver
- ServiceDesk (brugerstøtte)
- Teknisk sikkerhed
- At stille netværks- og telefoniydelser (WAN/LAN) til rådighed
- Telefoni-infrastruktur, telefoniforsyning, herunder sammenhæng til tjenester i det offentlige telenet (mobil- og fastnet)
- Fjernadgang til PC-arbejdspladser
- Teknisk støtte til enheder på netværket (PC'er, printere mv.)
- Indkøb af it-udstyr og basissoftware.
- Distribution af it-programmer til differentierede arbejdspladser
- Koordinering til eksterne it-leverandører og andre eksterne it-aktører
- Styring af it-teknisk arkitektur, inklusive telefoni
- It-faglig rådgivning og støtte.

IT-Forsyningen omfatter ovenstående opgaver uanset ejerforhold til udstyr og programmel.

3.2 Kontrolmiljø, risikovurdering og monitorering

IT-Forsyningens kontrolmiljø reflekterer den stilling, som ledelsen har taget til betydningen af kontroller og den vægt, der lægges på kontroller i politikker, procedurer, metoder og organisatorisk struktur. Følgende er en beskrivelse af IT-Forsyningens kontrolmiljø angående IT-Forsyningen og leverancer af it-services:

- Ansvar, IT-Forsyningens direktion og bestyrelse
- Tværgående samarbejdsmodel
- IT-Forsyningens organisationsstruktur
- Human Resources politikker og praksis
- Risikostyring
- Overvågning.

3.2.1 Ansvar, IT-Forsyningens direktion og bestyrelse

Bestyrelsen mødes ca. fem gange årligt for at drøfte forhold i forbindelse med driften af IT-Forsyningen og for at gennemgå økonomien, herunder forretningspolitikker

Bestyrelsesmedlemmerne er hver især underlagt de respektive kommunalbestyrelsers instruktionsbeføjelse. Formandskabet varetages på skift for to år ad gangen. Allerød Kommune har haft formandskabet i perioden fra 1. januar 2020. Fra 1. januar 2022 overtager Egedal Kommune formandskabet. Hver af interessenterne har udpeget ét bestyrelsesmedlem fra direktionen samt én personlig suppleant fra direktionen.

Bestyrelsen består for nuværende af bestyrelsesformand Morten Knudsen, kommunaldirektør i Allerød Kommune, Eik Møller, kommunaldirektør i Ballerup Kommune, Christine Brochdorf, kommunaldirektør i Egedal Kommune og Steen Vinderslev, kommunaldirektør i Furesø Kommune. Direktøren for IT-Forsyningen, Rasmus Winther, er sekretær for bestyrelsen, jf. vedtægterne.

Revisionsselskabet Deloitte udfører finansiel revision af IT-Forsyningen I/S i forbindelse med aflægning af årsregnskab 2021.

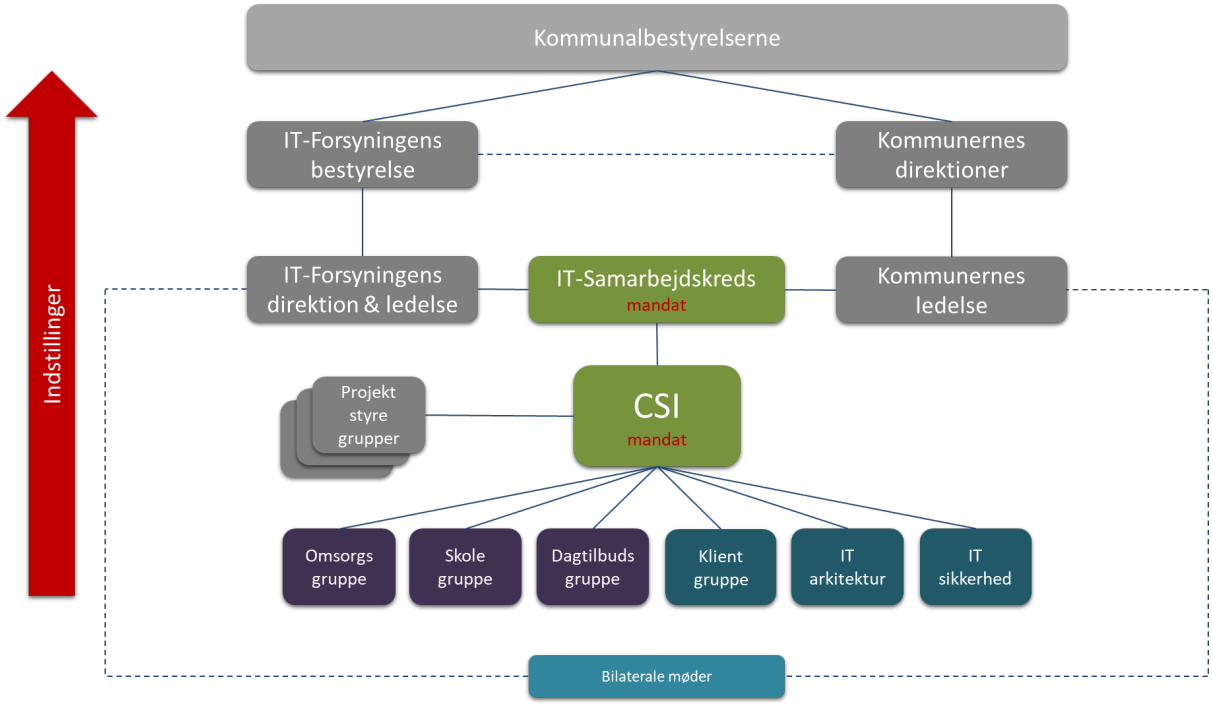
Der foreligger ingen sagsanlæg mod IT-Forsyningen.

3.2.2 Tværgående samarbejdsmodel

For at sikre dialog og kommunikation på tværs mellem IT-Forsyningen og de fire ejerkommuner, er der etableret en samarbejdsmodel, der med IT-Samarbejdskredsen i centrum har til hensigt at imødekomme og tilgodese flere faglige niveauer og derved sikre, at behovsformuleringer og fastlæggelse af fælles aktiviteter sker med afsæt i henholdsvis fagligt stærke og beslutningsdygtige fora.

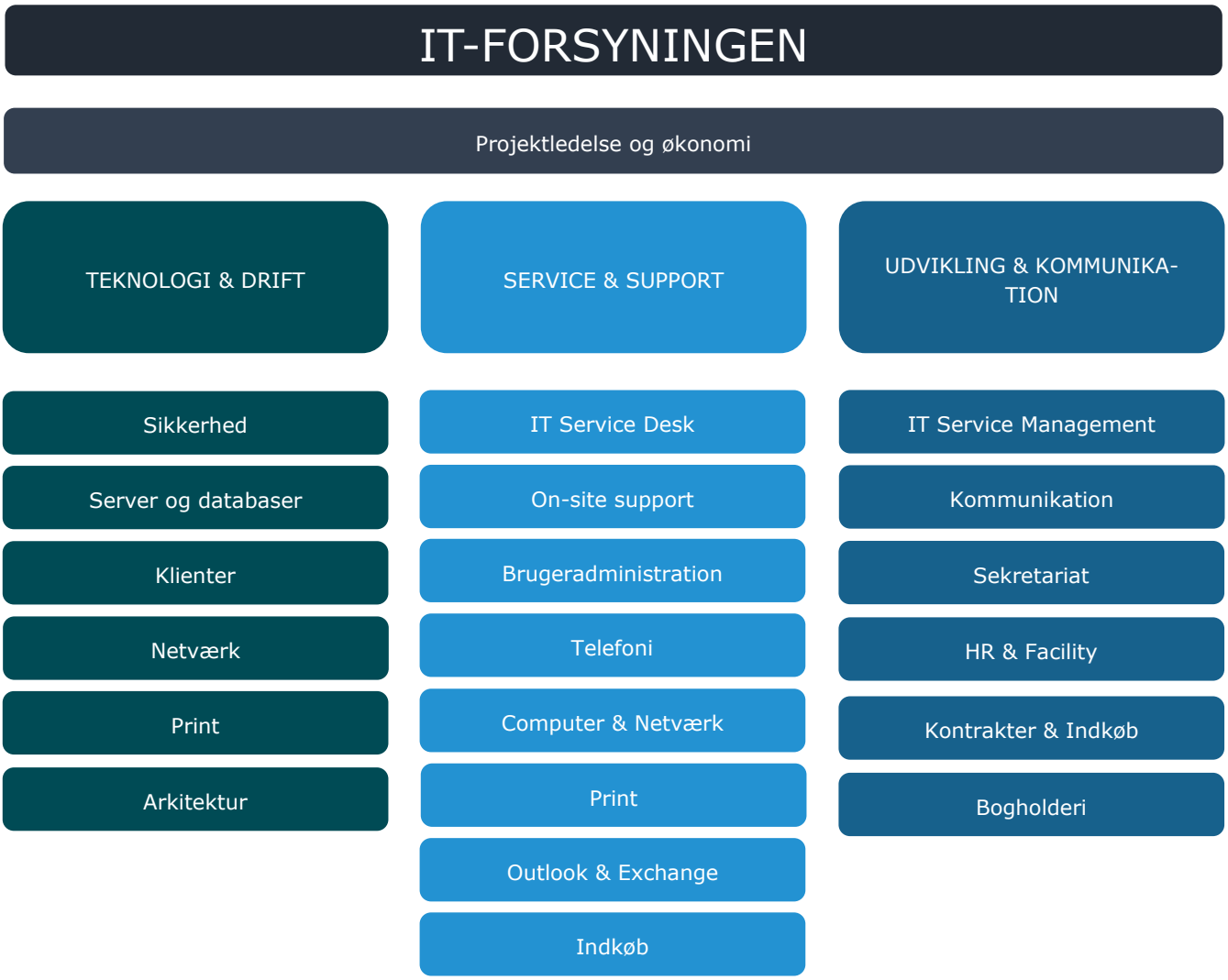
Alle fora er samarbejdsfora, hvor de deltagende personer forventes aktivt at involvere sig og sikre fremdrift. Samtidig skal deltagerne opsamle, behandle og afstemme idéer og behov fra ejerkommunerne og selskabet, så at indbyrdes afhængigheder koordineres.

Modellen har således til hensigt at sikre, at der sigtes efter økonomiske potentialer, serviceløft og kvalitet ved en fokuseret, koordineret og tværfaglig indsats, der tilgodeser forretningens behov og falder i tråd med de overordnede strategier, der ligger for området.



IT-Samarbejdskredsen er et samarbejdsudvalg med mandat til at godkende, igangsætte og initiere bevilling til fælles tiltag, herunder principper for økonomi og afregning, investeringsplan og prioritering samt opfølgning på strategiske fokusområder. CSI-kredsen er et samarbejdsudvalg med mandat til at igangsætte og drive initiativer om ensartede løsninger og koordinering af tværgående aktiviteter. Kredsenes deltagere har således de nødvendige beføjelser til at repræsentere ejerkommunerne og sikre en ensartet beslutningsproces på tværs, herunder den bagvedliggende beslutning og tilhørende økonomi i ejerkommunerne. CSI-kredsen er ejer af IT-Forsyningens servicekatalog og IT-Samarbejdskredsen ejer styringsgrundlaget.

De øvrige underliggende grupper er arbejdsgrupper, der har til ansvar at koordinere og drive igangsatte initiativer mv. Deltagerne i disse grupper har således de rette kompetencer og beføjelser til at udvælge, anbefale og indstille kvalificerede beslutninger til godkendelse i CSI-kredsen og IT-Samarbejdskredsen.



3.2.3 IT-Forsyningens struktur

Nedenfor følger en beskrivelse af IT-Forsyningens samlede organisation.

IT-Forsyningens organisationsstruktur

IT-Forsyningen er organiseret i tre afdelinger, Service & Support, Drift & Teknologi og Udvikling & Kommunikation. Service & Support og Udvikling & Kommunikation ledes af service- og udviklingschef Helle Friis. Drift & Teknologi ledes af direktør og driftschef Rasmus Winther.

IT-Forsyningen knytter en kontaktperson til hver opgave, der bestilles, og vedkommende har sammen med ejerkommunen ansvaret for at levere det aftalte.

I udgangspunktet varetages Service Center, udkørende support samt Service Management af afdelingen Service og Support. Technical Management og IT Operations Management varetages i afdelingen Drift og Teknologi.

3.2.4 Human Resources politikker og praksis

Ansættelsespraksis for IT-Forsyningen er standardiseret og dokumenteret. Denne praksis forudsætter, at lederen udarbejder et stillingsopslag og fremsender den til godkendelse hos direktøren. Når godkendelsen foreligger, vil stillingen opslås som ledig, inkl. stillingsbeskrivelsen. Ansøgningerne gennemses med

henblik på minimumskvalifikationer, og samtaler afholdes. Tilbud om ansættelse vil afhænge af referencer og baggrundstjek.

HR-politikker og procedurer ligger i IT-Forsyningens dokumentarkiv i Projectplace. Disse politikker omfatter, men er ikke begrænset til, følgende:

- Lokalaftaler om arbejdstider, vagtordning og MED-udvalg
- Politikker for alkohol, rygning og sygefravær
- Retningslinjer for anskaffelser og godkendelser samt indberetning af ferie og sygdom
- Oversigt over personalegoder og -politikker
- Regelsæt for gaver og deltagelse i arrangementer
- Instrukser om arbejdsudførelse, herunder incident, change og problem management.

Alle nyansatte i IT-Forsyningen bliver af leder instrueret i IT-Forsyningens politikker og -aftaler samt generelle driftspraksis.

Ansatte har ret til fem ugers årlig ferie samt en 6. uges ferie. Heraf kan tre ugers ferie afholdes i hovedferien. Den ansattes leder skal godkende ferieafholdelse. På dagen efter Kristi Himmelfart samt i dagene mellem jul og nytår holder IT-Forsyningen lukket.

Den ansvarlige leder holder årligt medarbejderudviklingssamtaler (MUS) med hver medarbejder. Samtalerne er en åben og ligefrem dialog mellem medarbejder og leder. Formålet med medarbejderudviklingssamtalerne er at skabe grundlag for, at den enkelte medarbejder trives og fungerer, men også at medarbejderen og jobbet udvikler sig sammen og i overensstemmelse med begge parters ønsker og behov. Samtalerne tager udgangspunkt i et standardsamtaleskema, der er forberedt af medarbejder og leder forinden mødet.

Ved fratrædelse deaktiveres nøglekort samt fysiske og logiske sikkerhedsadgange og udstyr tilbageleveres. Tjekliste for ophør følges af ansvarlig leder.

3.3 Risikovurdering og overvågning

3.3.1 Risikovurdering

Ledelsen mødes ugentligt for at diskutere bl.a. forretningsrisici, inklusive økonomiske og teknologiske risici. Ledermøder gennemføres efter et månedshjul. 1. møde i hver måned omhandler HR samt licens- og leverandørporteføljestyring, 2. møde er om status på projekter, 3. møde omhandler sikkerhed og på 4. møde foretages økonomiopfølgning. Herudover har hvert ledermøde faste punkter omkring status fra afdelingerne og incident managers samt hver anden uge status fra teamledere.

Der afholdes månedligt personalemøder for alle medarbejdere, hvor der orienteres om og drøftes forhold omkring virksomhedens drift og udvikling.

Identificerede risici af væsentlig betydning for virksomhedens drift tages uden ugrundet ophold op i virksomhedens bestyrelse. Bestyrelsen er tillige ansvarlig for godkendelse af IT-Forsyningens informationssikkerhedspolitik og risikovurdering.

IT-Forsyningen indgår i dialog med ejerkommunerne omkring udarbejdelser og tilpasning af deres it-sikkerhedspolitikker, så snitflader mellem ejerkommunernes og IT-Forsyningens roller og ansvar afklares og defineres. Der er etableret en tværgående informationssikkerhedsgruppe med deltagelse af IT-Forsyningens og ejerkommunernes informationssikkerhedskoordinatorer. Gruppen mødes seks til syv gange om året.

3.3.2 Overvågning

3.3.2.1 Overvågning af driften

Der forefindes formelle ledelsesinformations- og rapporteringssystemer, der sikrer, at ledelsen kan overvåge nøglekontrol- og performancemål. Der er for udvalgte områder etableret overvågning af processer, økonomi og kvalitet. Rapporter gennemgås i forhold til relevans for målgruppen på ugentlige ledermøder, på bestyrelsesmøder, i IT-Samarbejdskredsen, CSI samt præsenteres på personalemøder.
Der udsendes ugentlige leverancerapporter for udvalgte SLA'er til IT-Forsyningens medarbejdere og ejerkommuner. På team-, afdelings- og personalemøder følges op på mål og fremdrift på SLA'er.

3.3.2.2 Overvågning af samarbejde

I de forskellige samarbejdsudvalg, jf. den tværgående samarbejdsmodel, drøftes kvaliteten af IT-Forsyningens leverancer.

Service- og supportchefen samt driftschefen afholder endvidere periodiske statusmøder med hver af ejerkommunerne. På statusmøderne drøftes projektstatus, driftsstatus og kundetilfredshed.

3.3.2.3 Overvågning af generelle it-kontroller

IT-Forsyningens ledelse afholder periodisk ad hoc møder internt og med ejerkommunerne, hvor it-sikkerhed kan være et emne på lige fod med drift og projektfremdrift. Under disse punkter drøftes relevansen og effektiviteten af de generelle it-kontroller og it-sikkerhedsniveauet, som IT-Forsyningen har designet og implementeret for at adressere de risici, som IT-Forsyningen og ejerkommunerne står overfor, ligesom behovet for implementering af yderligere kontroller samt modifikation af eksisterende kontroller vurderes.

Der er endvidere formelt etableret interne ledelsestilsyn i forbindelse med tilrettelæggelse af IT-Forsyningens regnskabsvæsen.

3.4 Information og kommunikation

3.4.1 Generelle it-kontroller

Generelle it-kontroller udgør det kontrolmiljø, hvor samtlige it-services drives. Derfor har det generelle it-kontrolmiljø indvirkning på effektiviteten af kontroller i applikationer, inklusive de kontroller, som ejerkommunerne bruger i forbindelse med levering af services fra IT-Forsyningen.

I afsnit 3.6 beskrives de generelle kontroller relateret til IT-Forsyningen:

- Applikationsdrift
- Drift af WAN og dataring
- It-infrastruktur
- Sikkerhed - Fysisk adgang
- Sikkerhed - Logisk adgang
- Ændringskontrol
- Sikkerhed – datacenter infrastruktur og miljø.

3.4.2 Kommunikation

3.4.2.1 Ansatte

IT-Forsyningen har implementeret forskellige kommunikationsmåder for at hjælpe deres ansatte med at forstå deres individuelle roller og ansvar, selskabskontroller og for at hjælpe dem med at sikre, at væsentlige hændelser kommunikeres i tide. Disse omfatter:

- Orientering af nyansatte og eksisterende ansatte, der ændrer jobfunktion. Der lægges kursusplaner, for at medarbejderne kan håndtere ændringer i teknologi og politikker. Nyansatte gennemgår IT-Forsyningens politikker som en del af orienteringsprocessen
- Information til medarbejderne om væsentlige hændelser og ændringer til selskabspolitikker via notater, der udgives i Projectplace. Information, hvor tiden spiller en rolle, kommunikeres til ansatte via e-mails
- Personalemøder, der afholdes en gang månedligt. Og efter behov holdes møder med den enkelte medarbejder. Disse møder giver den ansatte mulighed for at bringe spørgsmål eller undtagelser til standardpolitik, som de måtte have, til ledelsens kendskab
- Afdelingsmøder i de tre afdelinger ugentligt, hvor konkrete faglige emner, nye tiltag, processer, organisatoriske, administrative samt sikkerhedsmæssige forhold kommunikeres og drøftes.

3.4.2.2 Ejerkommunerne

IT-Forsyningen har indført flere kommunikationskanaler for at sikre, at ejerkommunerne forstår IT-Forsyningens roller og ansvar og for at sikre, at hændelser bringes til ejerkommunernes kendskab hurtigst muligt. Disse metoder inkluderer ejerkommunernes aktive deltagelse i samarbejdsfora, dialogmøder, samt ledere og medarbejdere, der holder kontakten med ejerkommunernes repræsentanter for at holde hinanden informeret om nye emner og udviklingen.

Kommunikationen med ejerkommunerne varierer fra område til område. Imidlertid holdes ejerkommunerne orienterede om systemændringer, der kan have indflydelse på kommunens organisation via statusmøder, e-mail- eller SMS-varslinger. Tillige har IT-Forsyningens ledelse regelmæssigt kontakt med ejerkommunernes digitaliseringsafdelinger via personlige møder, telefon, SMS og e-mail. Ved driftsforstyrrelser kommunikeres der løbende til den/de berørte ejerkommuner i form af notifikationer på forsiden af IT Service Desk. Information om driftsforstyrrelser og decideret krisekommunikation kommunikeres tillige til udpegede personer via gruppe-SMS.

3.5 Oversigt it-services

3.5.1 Servicekatalog

IT-Forsyningen har i samarbejde med repræsentanter fra ejerkommunerne udarbejdet et servicekatalog, der beskriver de services, som IT-Forsyningen leverer til ejerkommunerne. IT-Forsyningen benytter en servicebaseret forretningsmodel, som indebærer:

- At samtlige services (materielle som immaterielle) beskrives
- At der styres efter SLA
- At et servicekatalog benyttes
- At en bestillingsportal, hvor kommunen kan bestille og afbestille it-services, benyttes
- At der tages betaling for de services, der leveres, enten gennem direkte betaling eller forskellige former for abonnement.

Hos IT-Forsyningen arbejdes der med et servicekatalog, der er brugervendt. Det er offentligt og indeholder de services, som IT-Forsyningen tilbyder ejerkommunerne. Servicekataloget er p.t. i version 4.

IT-Forsyningen har en forsynings- og serviceforpligtelse i forhold til flere målgrupper:

1. Brugere på det administrative net:
   Medarbejdere med en brugerkonto og som typisk har adgang til en PC og en række administrative programmer
2. Brugere på det pædagogiske net:
   Lærere, pædagoger, it-vejledere og elever på ejerkommunernes skoler, som bruger programmer, der anvendes i den konkrete undervisning (servicekataloget beskriver, hvad der serviceres)
3. Brugere på det offentlige netværk (hot spots):
   Kan være borgere på biblioteket, i borgerbetjeningen, på jobcentrene eller personer, der anvender

deres eget udstyr. Her yder IT-Forsyningen alene adgang til netværket og kun service til 'kommunale enheder' på netværket, ikke borgernes egne enheder.

Nedenstående liste viser, hvilke services der er beskrevet og godkendt:

Support og rådgivning
- Service Center
- Bestillinger (varekøb)
- Brugeradministration (ADM)
- Brugeradministration IDM (Skole)
- PC-vedligehold
- Fjernopkobling
- E-mail
- Microsoft Visio og Project
- Print, scan og kopi
- Chromebook Management (skole)
- Styring af mobile enheder (MDM/EMM)
- Telefoni Fastnet
- Projekter og projektledelse
- Rådgivning
- VIP-servicevagt.

Fysiske enheder/IT-arbejdsplads
- Standard-PC (administrativ)
- OS2 Borger PC
- Standard-PC (skole)
- Standard-PC (dagtilbud)
- Special PC
- PC-tilbehør
- Chromebook (skole)
- Mobiltelefon og smartphone
- Tablet
- Printer og multifunktionsprinter.

Systemer og data
- Applikationsadgang
- Backup og genetablering
- Certifikatadministration
- Føderation (IdP).

Drift, servere og netværk
- Netværksdrift
- Server- og applikationsdrift
- Applikationsdrift (inkl. serverdrift)

I det følgende er uddrag af beskrivelsen på et par eksempler på it-services.

Service Center
IT-Forsyningens Service Center er det primære kontaktpunkt ved fejlmeldinger og bestillinger. IT-Forsyningens Service Center kan kontaktes telefonisk eller ved at oprette en henvendelse i IT Service Desk. Henvendelser registreres som sager (incidents) i IT Service Desk og kan udgøre fejl på udstyr, driftsfejl, anmodning om brugersupport eller status på aktive incidents etc. Medarbejderne i Service Center registrerer enhver henvendelse og vil, i det omfang henvendelsen drejer sig om kendte fejl, almen brugersupport og/eller status på igangværende supportsager, søge at løse opgaven med det samme. Er der

tale om mere komplicerede henvendelser, vil medarbejderne i Service Center kvalificere, prioritere og visitere og prioritere opgaven til rette fagteam i IT-Forsyningen.

Standard-PC (administrativ)
Denne service omfatter levering af en standard-PC til en administrativ bruger inklusive, kommunens valgte standardprogrammer. En standard-PC kan være en stationær eller en bærbar PC. PC'en ejes af IT-Forsyningen, og servicen inkluderer løbende opdateringer. For at sikre så høj en driftsstabilitet og mindske risikoen for funktionsfejl forårsaget af brugeren kan funktioner på PC'en være låst af IT-Forsyningen.

PC-vedligehold
Servicen omfatter sikkerhedsopdatering af Standard- og Special-PC'ere leveret af IT-Forsyningen, herunder antivirus, patchinstallation og -opdatering samt drift af adgangs- og rettighedsstyringssystemer (se Brugeradministration).

E-mail
Servicen giver adgang til e-mail og kalender på en sikker og pålidelig måde, når der findes netværksadgang-/internetadgang.

Backup og genetablering
Servicen omfatter pålidelig, automatisk backup-funktionalitet af data på fildrev samt servere under IT-Forsyningens drift, inklusive mulighed for genetablering af data. En backup foretages hver dag i tidsrummet kl. 18:00-06:00.

Alle servicebeskrivelser indeholder følgende elementer:
- Beskrivelse
- Målgruppe
- Serviceniveau/SLA
- Afgrænsning
- Forudsætninger for brug af ydelsen
- De enkelte elementer inkluderet i ydelsen
- Tilvalg (med eller uden betaling)
- Hvordan bestilles, ændres eller afmeldes service?
- Hvordan afregnes ydelsen, og er den indeholdt i basis?

3.5.1.1 Ejerkommunernes ansvar

IT-Forsyningens styringsgrundlag og servicekatalog beskriver snitfladerne til IT-Forsyningens services, herunder hvor og hvad ejerkommunernes ansvar er i forhold til bestilling og afmelding af services, egen drift og informationskrav til IT-Forsyningen. Et par af de vigtige snitflader i forhold til ansvarsdelingen med relation til it-sikkerhed er beskrevet i dette afsnit.

IT-Forsyningen er driftsleverandør for ejerkommunerne og foretager prioriteringer i sagsløsningen i relation til kommunernes egne prioriteringer af data og systemer. Ejerkommunerne har derfor ansvaret for at etablere deres egne kontroller for klassificering af information og systemer. IT-Forsyningen efterspørger denne klassifikation hos ejerkommunerne én gang årligt.

El- og svagstrømsforsyning samt netværkskabling er ikke en del af de services, der leveres fra IT-Forsyningen. Disse services tilhører bygningers vedligehold. Hvis en bygning er lejet, er det en relation mellem lejer og ejer, som skal etablere elforsyning, netværkskabling, svagstrøm og stik efter de specifikationer/anbefalinger, der foreligger. Fysisk sikring af kommunens egne kontorer og lokaler, herunder adgangskontrol, falder under kommunens ansvarsområde.

IT-Forsyningen yder ikke support til anvendelsen af it-fagsystemer, men sikrer alene, at de aftalte enheder, netværk og programmer er tilgængelige. Ansvaret for de nødvendige rettigheder i et fagsystem ligger hos den enkelte systemejer. Brugeradministration foretages for ejerkommunerne efter en bestiller-

udfører model. Det er derved ejerkommunernes ansvar at have egne kontroller og processer i forhold til onboarding og offboarding samt ændring af rettigheder for kommunens brugere og bestille dette udført hos IT-Forsyningen. Periodiske gennemgange af kommunens brugere og rettigheder påhviler desuden kommunen.

Logning af adfærd i fagsystemer er kommunernes systemejeres ansvar. IT-Forsyningen foretager logning af infrastruktur samt backup af data på servere, databaser og fildrev, der driftes i eget datacenter. IT-Forsyningen tilbyder en standardkonfiguration af backup, som er beskrevet i servicebeskrivelsen, og som er aftalt med ejerkommunerne via arbejdet med og godkendelse af servicekataloget.

IT-Forsyningen har ikke overtaget kommunens informationssikkerhedspolitik, da denne påhviler den enkelte kommune. Det er således den enkelte kommunes ansvar at sikre, at IT-Forsyningen har den nødvendige viden herom, herunder at kommunikere konfigurationskrav til adgangskoder. IT-Forsyningen foretager udtræk af opsat adgangskodepolitik på kommunens domæner årligt og indhenter godkendelse heraf hos kommunens it-sikkerhedskoordinator.

3.5.1.2 Implementering

Anskaffelser i IT-Forsyningen følger en fastlagt proces. Alle varer, licenser og øvrige ydelser/aftaler, der anskaffes til eller indgås hos IT-Forsyningen med henblik på at indgå i drift og leverance, skal godkendes af nærmeste leder. Det vil sige, at der indhentes godkendelse for anskaffelse hos lederen eller dennes stedfortræder. Ved større anskaffelser er denne godkendelse altid skriftlig. Småanskaffelser, så som nødvendige stumper eller klip på indkøbte klippekort, kan godkendes mundtligt. Afdelingsledere kan godkende indkøb på op til 10.000 kr. Øvrige indkøb samt abonnementsaftaler godkendes af IT-Forsyningens direktion. Opsigelse/ændring af eksisterende aftaler følger samme procedure.

Drifts- og teknologichefen er gatekeeper i forhold til implementering af nye løsninger. Det indebærer, at systemer, der idriftsættes i IT-Forsyningens driftsmiljø, skal være accepteret af denne på baggrund af en faglig vurdering. Change manageren er ansvarlig for change management og formand for CAB-udvalget, der mødes ugentligt. CAB-udvalget består af change manager og ledelsen i IT-Forsyningen med ad hoc-indkaldelse af "change-bestillere". I CAB vurderes ændringer og idriftsættelser, der kan have betydning for IT-Forsyningens drift på baggrund af kritikalitet, konsekvenser for brugere, tidssammenfald mellem ændringer og niveauet af kommunikation til brugere og ejerkommuner mv.

3.6 Processer og kontroller

Der foreligger forretningsgange og arbejds- og kontrolbeskrivelser på udvalgte områder. De enkelte kontrolmål og kontrolaktiviteter, der understøtter nedenstående processer og kontroller, fremgår af sektion 4.

3.6.1 Applikationsdrift

Backup er inkluderet i applikationsdrift og PC-ydelsen. Dette sikrer beskyttelse af ejerkommunernes kritiske data, når det drejer sig om integritet og sikkerhed. Sikkerhedskopier tages hver nat gennem en automatisk disk til disk-backupproces. Sikkerhedskopierne lagres på dedikeret backuplager i andet datacenter end det primære datacenter, hvor applikationsdrift og datalagring foretages. Der foretages på hverdage kontrol af status på forudgående sikkerhedskopiering. Det er aftalt med ejerkommunerne, at sikkerhedskopier gemmes i 60 kalenderdage for dokumentdrev- og databaser. Sikkerhedskopier gemmes i 14 kalenderdage for alle andre servere, herunder mail- samt fagsystemer. Der gennemføres periodisk gendannelse af en tilfældig udvalgt server, så det kontrolleres, at indhold af sikkerhedskopiering er validt.

3.6.2 Drift af WAN og dataring

TDC tilvejebringer højhastigheds-fiberforbindelse mellem de fire netværksknudepunkter og datacentre i en redundant dataring. I Allerød og Ballerup Kommune er kommunens lokationer forbundet via MPLS-kredsløb leveret af TDC. Ballerup Kommune omlægger udvalgte strækninger til egen fiber i takt med at

denne nedgraves. I Furesø Kommune leveres forbindelser mellem lokationer på egen fiber og via fiber og xDSL-forbindelser fra GlobalConnect. I Egedal Kommune leveres WAN-forbindelserne via fiber fra TDC, egne fibre samt via fiber og air-fiber fra GlobalConnect.

IT-Forsyningen ejer leverance- og servicekontrakterne på linjeleje og foretager periodisk opfølgning herpå.

3.6.3 It-infrastruktur

3.6.3.1 Datacenter topologi

IT-Forsyningens primære datacenter er placeret hos Ballerup Kommune, og backup-datacenteret er placeret hos Allerød Kommune. Endvidere forefindes datacentre, der fungerer som netværksknudepunkter hos Egedal Kommune og hos Furesø Kommune.

IT-Forsyningens datacenter anvender følgende hardware:

- Server- og applikationsdrift leveres i virtuelt datacenter baseret på VMware med computing og storage leveret på hyperconverged-miljø fra Cisco
- Fiberswitches i datacenteret er fra henholdsvis Cisco og HP
- Firewalls mellem de fire kommuner og IT-Forsyningen er under omlægning fra HP-udstyr til Checkpoint.
- Firewalls mellem ejerkommunerne og internettet er under konsolidering til CheckPoint. Et enkelt miljø på Palo Alto udestår i omlægningen.

3.6.3.2 Datacenter netværksinfrastruktur

IT-Forsyningen samarbejder med TDC, der leverer sort fiber, for at levere driftsstabile, fuldt ud skalerbare links mellem ejerkommunernes centrale netværksknudepunkter og til IT-Forsyningens datacentre.

3.6.3.3 Serverplatform

IT-Forsyningens virtuelle servermiljø er opbygget omkring 26 compute- og storagenoder.

3.6.3.4 Backup

IT-Forsyningens backupløsning er en remote disk til disk-backupløsning baseret på Cisco UCS, der fysisk er placeret i vores datacenter i Allerød.

3.6.3.5 Driftsovervågning

Der forefindes formelle ledelsesinformations- og rapporteringssystemer, der sikrer, at ledelsen kan overvåge nøglekontrol- og performancemål. IT-Forsyningens ledelse etablerer og vedligeholder standarder for udvalgte driftsovervågningsområder. Der opsættes primært automatiske systemer og manuelle systemer, hvor automatik ikke kan leveres, der leveres overvågning af udvalgte områder. Den enkelte afdelingschef er ansvarlig for ledelsesinformationen fra de processer, de er ansvarlige for.

Der er etableret systemer til overvågning af servere og systemer. Systemer kategoriseret af ejerkommunerne som meget kritiske systemer overvåges 24x7 for oppetid, tilgængelighed, diskplads og services. Hvis kritisk niveau nås, eller udfald registreres, alarmeres IT-Forsyningens teknikere og rådighedsvagter via SMS.

3.6.4 Sikkerhed – fysisk adgang

IT-Forsyningen har etableret formelle politikker og procedurer for adgangskontrol til systemer, faciliteter og datacentre. Informationssikkerhedspolitikken beskriver det ledelsesgodkendte niveau for sikkerhed. Dermed skal politikken ligeledes understøtte bevidstheden om informationssikkerhed i IT-Forsyningens

organisation og funktion. De politikker og procedurer, der udformes for at understøtte informationssikkerhedspolitikkens hovedmålssætninger, skal sikre, at alle medarbejdere arbejder med og forholder sig til informationssikkerhed i det daglige arbejde.

3.6.4.1 Administration af adgangskontrol

Adgangen til datacentrene er sikret af elektroniske læsere af adgangskort, som er forbundet med centralt adgangskontrolsystem. Adgang til datacentrene gives ud fra jobansvar af IT-Forsyningens ledelse og administreres af udvalgt sikkerhedspersonale i hhv. Ballerup, Furesø, Allerød og Egedal Kommune. Sikkerhedsadministratoren skal kræve, at IT-Forsyningens ledelse autoriserer adgang, før kort udarbejdes og udleveres. IT-Forsyningen rekvirerer periodisk lister over medarbejdere med adgang til datacentrene og anmoder sikkerhedsadministratoren om justering af brugeradgange. Ansvarlig leder i IT-Forsyningen har ansvar for at afmelde adgange til datacentre ved medarbejderes ansættelsesophør.

3.6.4.2 Overvågning

Adgange til datacentre er udstyret med alarmer. Kommunernes rådhuse, hvor datacentrene er placeret, overvåges ved perimeteren med videokameraer. Kommunernes vagtpersonale undersøger aktivering af døralarmer. Sikkerhedsvagter konfronterer alle uautoriserede eller mistænkelige personer, som forsøger at få adgang uden for normal arbejdstid. Eksterne konsulenter og entreprenører, der har behov for at servicere udstyr i datacentre, skal være i følge med medarbejder fra IT-Forsyningen under opholdet i datacenteret.

3.6.5 Sikkerhed – logisk adgang

3.6.5.1 Ansvar for logisk adgang

IT-Forsyningen har ansvar for at udvikle standarder og administrere logisk sikkerhed for personale på udvalgte systemer og applikationer. Kommunernes applikationsmiljøer er adskilt fra hinanden, hvis der ikke er aftalt og etableret fælles løsning i det delte domæne. Oprettelse og nedlæggelse af administrative rettigheder til ejerkommunernes brugerdomæner udføres for IT-Forsyningens ansatte af IT-Forsyningens brugeradministration og kræver autorisation af leder i IT-Forsyningen. Oprettelser og nedlæggelser dokumenteres i IT-Forsyningens sagsstyringssystem.

IT-Forsyningen tildeles ikke administrative rettigheder til ejerkommunens fagsystemer. I enkelte fagsystemer kan IT-Forsyningens medarbejdere, af ejerkommunens systemejere, tildeles loginadgang med minimale rettigheder med det formål at kunne teste og overvåge den specifikke applikations installation og tilgængelighed.

3.6.5.2 Logisk sikkerhedskontrol

Kommunernes personale såsom systemejere og leverandører kan have behov for at få adgang til servere og systemer for vedligeholdelse og support. Dette gøres muligt gennem flere niveauer af logisk sikkerhed og godkendelsesprocesser. Det er obligatorisk for IT-Forsyningens og ejerkommunernes personale og leverandører at anvende personligt bruger-id og adgangskode, samt at have bestilt med rette autorisation og tildelt adgang til det specifikke system og/eller server. For eksterne leverandører gælder desuden, at der skal være indgået fortrolighedserklæring og eventuelt databehandleraftale.

Bruger-id og adgangskoder til netværk, platform og de fleste applikationer har interne indstillinger, der tillader et foruddefineret antal ugyldige adgangsforsøg, før de deaktiveres. Adgang kan genaktiveres ved henvendelse til IT-Forsyningens Service Center, hvor aftalt procedure følges for genåbning.

IT-Forsyningen har fastlagt krav til adgangskoder i adgangskodepolitik.

I ejerkommunernes brugerdomæner er aktiveret de adgangskodepolitikker, som ejerkommunerne har vedtaget i egne sikkerhedspolitikker. Der sker årlig opfølgning på, om de aktiverede politikker modsvarer kommunernes vedtagne standard.

3.6.5.3 Logning

Der er etableret logning af brugeraktivitet, undtagelser og fejl på servere og databaser. Logning gennemgås reaktivt ved behov og ved mistanke om uregelmæssighed. Logoplysninger opbevares på servere, så det kræver specifikt tildelte rettigheder at tilgå logge.

Der er etableret central logningsfunktionalitet, hvor der opsamles hændelseslogning af sikkerhedslogs vedrørende brugeraktivitet og rettighedstildeling samt undtagelser og fejl fra system- og applikationslogs fra alle domain controllere på domæner håndteret af IT-Forsyningen. For væsentlige områder sendes besked om nødvendig gennemgang af sikkerhedslogs til udvalgte teknikere. Drift- og Teknologichef fastlægger områder og opfølgning.

IT-Forsyningens hovedfokus for logmanagement er drift af infrastrukturen. Logopsamling og –opfølgning fra fagsystemer hører under ejerkommunernes ansvar.

3.6.6 Ændringskontrol

Alle ændringer er underlagt og udføres i henhold til IT-Forsyningens change-procedure, hvis formål er at sikre, at ændringer i IT-Forsyningens driftsmiljø gennemføres i henhold til de aftalte rammer med mindst mulige gener for brugerne. Ændringer beskrives og udføres i henhold til nedenstående:

- Der foretages registrering af changes i Cherwell, herunder type af change
- Datakvalitet kontrolleres og udfyldes om nødvendigt, så change er klar til vurdering
- Change vurderes, og anbefalinger om videre fremdrift skrives ind
- Change godkendes af CAB eller en anden relevant Change Authority (typisk change manager)
- Change udføres på et forud aftalt tidspunkt af changebestiller
- Change kontrolleres for, om aktiviteterne er gennemført med succes, og lukkes ned.

Change orders gennemgås på et ugentligt CAB-møde, hvor de faste deltagere er service- og supportchef, drifts- og teknologichef, change manager og eventuelt changebestillere.

3.6.7 Sikkerhed – datacenter infrastruktur og miljø

3.6.7.1 Fysiske sikringsforanstaltninger

IT-Forsyningens primære datacenter i Ballerup er forsynet fra elnettet via separat tavle til forsyning af datacenteret. Der er et nødstrømsanlæg (UPS), der øjeblikkeligt træder i kraft ved strømudfald på elnettet. UPS-anlægget sikrer oppetid indtil en dieselgenerator kan fortsætte den videre drift. Generatoren kan uden forsyning sikre oppetid i op til 16 timer fra et strømnedbrud. 24x7x365-aftale med serviceleverandør er etableret. Serviceleverandøren påfylder diesel ved eftersyn og ved bestilling. Generatoren kontrolleres, rengøres og test-startes fire gange årligt af serviceleverandøren.

Rackskabe er monteret i containmentløsning (Kuben), der sikrer optimalt airflow. Et redundant køleanlæg sørger for, at kølig, filtreret luft ”skubbes” op gennem rackskabet nedefra, via hævede, perforerede gulve. Alle rackskabe i Kuben har en temperatur på under 24°C. Temperaturen monitoreres, og der gives alarm via SMS, hvis temperaturen overstiger grænseværdi; advarsel ved over 26°C og alarm over 28°C.

Der er ligeledes opsat optiske og ioniserende røgalarmer i både loft og under det hævede gulv i lokalerne. Disse holder konstant øje med de lokaler, hvor udstyret fysisk er placeret, og afgiver alarm audiovisuelt.

Det område, der benyttes til placering af udstyr, er beskyttet af Argonite-anlæg, der er koblet til de ovenstående brandmeldeanlæg. Ved brand aktiveres det automatiske brandslukningsanlæg og samtidig sendes alarm til brandmyndighederne. Anlægget serviceres årligt af autoriseret ekstern leverandør.

Backupdatacenteret i Allerød samt hovedkrydsfelterne i Egedal og Furesø er forsynet via UPS samt holdes tilstrækkeligt tempereret af køleanlæg. Hovedkrydsfeltet i Egedal er forsynet via generator.
De to datacentre hovedrengøres to gange årligt af uddannet personale.

3.6.7.2 Antivirus og sikkerhedshændelser

Der er etableret antivirus på alle PC'er samt alle servere, som er opkoblet til central administrationskonsol. Antivirus er konfigureret til automatisk opdatering.

Webtrafik filtreres via ekstern leverandør, der blokerer for sider med potentielt skadevoldende indhold. Filtreringer er etableret for IT-Forsyningen og ejerkommunerne.

Der foretages virus-, malware- og spamscanning af alle indgående og udgående e-mails fra ejerkommunernes og IT-Forsyningens mailsystemer.

Sikkerhedshændelser opdages via monitorering eller brugernes indmeldinger, håndteres af udvalgte medlemmer af IT-Forsyningens personale og håndbæres igennem umiddelbart efter opdagelse er sket. Sikkerhedshændelser rapporteres til ledelse. Procedure herfor er beskrevet og fremgår af IT-Forsyningens sikkerhedshåndbog.

3.6.7.3 Bortskaffelse af medier

PC'er og andet udstyr bortskaffes forsvarligt i forhold til destruktion eller genanvendelse af udstyr, så eventuelle følsomme data slettes fra udstyr. Der er indgået aftale med ekstern leverandør herom.

3.6.7.4 Beredskabsplan

Der er etableret beredskabsplan for IT-Forsyningen, som vedligeholdes og testes årligt.

3.6.7.5 Vagtordning

IT-Forsyningen har i samarbejde med ejerkommunerne etableret en vagtordning, hvor teknikere står til rådighed 24x7x365. Rådighedsvagten kan varsles teknisk via SMS fra overvågningssystemerne eller telefonisk af brugere, der oplever serviceudfald på systemer kategoriseret som meget kritiske systemer.

4. Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf

4.1. Introduktion

Denne rapport er udformet med henblik på at informere kommunerne om IT-Forsyningens systemer og kontroller, som kan påvirke behandlingen af forretningsrelaterede transaktioner, og samtidig informere kommunerne om funktionaliteten af IT-Forsyningens kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i brugerorganisationernes forretningsprocesser, har til hensigt at hjælpe brugerorganisationens revisor til at (1) planlægge revisionen af brugerorganisationens årsregnskaber og (2) vurdere risici for fejl i årsregnskaber, som muligvis påvirkes af de generelle it-kontroller hos IT-Forsyningen.

Vores test af IT-Forsyningens kontroller er begrænset til de kontrolmål og tilknyttede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, som er beskrevet i systembeskrivelsen, eller til de generelle it-kontroller, som skal være implementeret i brugerorganisationerne for at opfylde kontrolmålene. Det er hver brugerorganisations revisors ansvar at evaluere denne information i forhold til de kontroller, som eksisterer i hver brugerorganisation. Hvis bestemte supplerende kontroller ikke er til stede i brugerorganisationerne, kan IT-Forsyningens kontroller muligvis ikke kompensere for sådanne svagheder.

4.2. Test af kontroller

De test, der udføres i forbindelse med fastlæggelsen af kontrollers funktionalitet, består af en eller flere af følgende metoder:

Metode	Beskrivelse
Forespørgsel	Forespørgsel hos udvalgt personale hos IT-Forsyningen
Observation	Observation af kontrollens udførelse
Inspektion	Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelsen af kontroller. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er udformet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol med henblik på at verificere, at kontrollen fungerer som forudsat

4.3. Test af kontrollernes funktionalitet

Vores test af kontrollernes funktionalitet inkluderer de test, som vi betragter som nødvendige for at vurdere, om de udførte kontroller og overholdelsen heraf er tilstrækkelige til at give høj, men ikke absolut sikkerhed for, at de specificerede kontrolmål blev opnået i løbet af perioden 1. januar 2021 - 31. december 2021.

Vores test af kontrollernes funktionalitet var udformet til at dække et repræsentativt antal af transaktioner i løbet af perioden 1. januar 2021 - 31. december 2021 for hver kontrol, jf. nedenfor, som er udformet til at opnå de specifikke kontrolmål. Ved udvælgelsen af specifikke test har vi overvejet (a) karakteren af de testede områder, (b) typerne af tilgængelig dokumentation, (c) karakteren af de revisionsmål, der skal opnås, (d) det vurderede kontrolrisikoniveau og (e) testens forventede effektivitet.

4.4. Kontrolmål, kontroller og resultater af test

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.5 – Informationssikkerhedspolitikker			
A.5.1 – Retningslinjer for styring af informationssikkerhed			
Formål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.			
5.1.1 Politikker for informationssikkerhed IT-Forsyningen har, med afsæt i en risikoanalyse, udarbejdet en ledelsesgodkendt informationssikkerhedspolitik, som er offentliggjort og kommunikeret til relevante medarbejdere og eksterne parter.	Ingen.	Inspiceret risikoanalysen med henblik på at konstatere, at denne var betryggende udformet, samt at denne var godkendt af ledelsen. Inspiceret informationssikkerhedspolitikken med henblik på at konstatere, at denne var betryggende udformet, samt at denne var godkendt af ledelsen. Inspiceret forretningsgang og anden dokumentation, der viser, at informationssikkerhedspolitikken kommunikeres til nye medarbejdere og nye eksterne konsulenter.	Ingen afvigelser konstateret.
5.1.2 Gennemgang af politikker for informationssikkerhed Risikoanalysen og informationssikkerhedspolitikken evalueres årligt eller ved væsentlige ændringer.	Ingen.	Inspiceret proceduren for periodisk gennemgang af risikoanalysen og informationssikkerhedspolitikken, og konstateret, at disse var godkendt af ledelsen i erklæringsperioden. Stikprøvevist inspiceret dokumentation for månedlige ledermøder med henblik på at konstatere, om informationssikkerhed behandles på disse.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.6 – Organisering af informationssikkerhed			
A.6.1 – Intern organisering			
Formål: At styre it-sikkerheden internt i organisationen.			
6.1.1 Roller og ansvarsområder for informationssikkerhed IT-Forsyningen har defineret og fordelt ansvarsområder for informationssikkerheden, samt kommunikeret dette til medarbejderne.	Ingen.	Observeret, at ledelsen har implementeret en it-sikkerhedsafdeling og har udpeget ansvarlige for informationssikkerheden. Forespurgt et udvalg af medarbejdere med henblik på at konstatere, om de var bekendte med ansvarsplaceringen for så vidt angår informationssikkerhed.	Ingen afvigelser konstateret.
6.1.2 Funktionsadskillelse Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Ingen.	Inspiceret den organisatoriske fordeling i IT-Forsyningen med henblik på at konstatere, om modstridende funktioner og ansvarsområder er adskilt for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.7 – Personalesikkerhed			
A.7.2 – Under ansættelsen			
Målsætning: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
7.2.1 Ledelsesansvar IT-Forsyningen afholder ugentlige ledermøder og månedlige personalemøder, hvorved det sikres, at ledere og medarbejdere er bekendte med informationssikkerheden.	Ingen.	Stikprøvevist inspiceret dokumentation for de ugentlige ledermøder og månedlige personalemøder med henblik på at konstatere, om informationssikkerhed behandles på disse.	Ingen afvigelser konstateret.
7.2.2 Bevidsthed om uddannelse og træning i informationssikkerhed Nyansatte orienteres om indhold i sikkerhedshåndbogen. Eksterne konsulenter skal underskrive fortrolighedserklæring. Der afholdes månedlige personalemøder, hvor medarbejdere holdes orienteret om informationssikkerheden.	Ingen.	Inspiceret, at sikkerhedshåndbogen opbevares på intranettet hos IT-Forsyningen, samt stikprøvevist forespurgt medarbejdere med henblik på at konstatere, om de er gjort bekendt med denne. Stikprøvevist inspiceret dokumentation for de månedlige personalemøder med henblik på at konstatere, om informationssikkerhed behandles på disse. Stikprøvevist inspiceret, at eksterne konsulenter underskriver en fortrolighedserklæring forud for, at de tildeles adgang til systemer og data.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.8 – Styring af aktiver			
A.8.1 – Ansvar for aktiver			
Formål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.			
8.1.1 Fortegnelse over aktiver Der vedligeholdes inventarlister over alle PC'er, servere og datalinjer samt diagrammer over netværksudstyr med væsentlige komponenter noteret. Inventarlister og diagrammer opdateres løbende. For PC'er foretages automatiserede opdateringer.	Det er ejerkommunernes ansvar at etablere kontroller for klassificering af egen information og systemer, samt kommunikere denne klassifikation til IT-Forsyningen med henblik på at opnå den korrekte overvågning, jf. klassificeringen.	Inspiceret, at der vedligeholdes oversigt over IT-Forsyningens og ejerkommunernes servere og systemer samt datalinjer. Inspiceret, at der vedligeholdes oversigt over de PC'er, som IT-Forsyningen drifter for ejerkommunerne. Inspiceret, at der vedligeholdes diagrammer over netværksudstyr.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.8 – Styring af aktiver			
A.8.2 – Klassifikation af information			
Formål: At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.			
8.2.3 Håndtering af aktiver Der er udarbejdet og implementeret procedurer til håndtering af aktiver i overensstemmelse med det informationsklassifikationssystem, som IT-Forsyningen sammen med ejerkommunerne har vedtaget.	Ingen.	Påset, at IT-Forsyningen har modtaget en klassifikationsoversigt over ejerkommunernes aktiver. Inspiceret proceduren for håndtering af aktiver med henblik på at konstatere, om aktiver håndteres i overensstemmelse med klassifikationsoversigten, som er udarbejdet af ejerkommunerne.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.9 – Adgangsstyring			
A.9.1 – Forretningsmæssige krav til adgangsstyring			
Formål: At begrænse adgangen til information og informationsbehandlingsfaciliteter			
9.1.1 Politik for adgangsstyring Der er udarbejdet en procedure vedrørende oprettelse og ændringer, tildeling af adgange og rettigheder, rettidignedlæggelse af brugere og periodisk revurdering af adgange og rettigheder.	Ingen.	Observeret, at der er udarbejdet en politik for adgangsstyring, samt at denne har været godkendt i hele erklæringsperioden.	Ingen afvigelser konstateret.
9.1.2 Adgang til netværk og netværkstjenester Medarbejdere tildeles udelukkende adgang til netværk og netværkstjenester, som de har et arbejdsbetinget behov for.	Ingen.	Observeret, at der er udarbejdet en politik for adgangsstyring til netværk og netværkstjenester. Stikprøvevist påset, at der i forbindelse med oprettelser tages stilling til, hvilke netværk og netværkstjenester der skal tildeles adgang til.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.9 – Adgangsstyring			
A.9.2 – Retningslinjer for styring af informationssikkerhed			
Formål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.			
9.2.1 Brugerregistrering og –afmelding Der er udarbejdet en procedure vedrørende oprettelse og ændringer, tildeling af adgange og rettigheder og rettidig nedlæggelse af brugere.	Ejerkommunerne har selv ansvaret for at kommunikere til IT-Forsyningen i forbindelse med oprettelse, ændringer samt nedlæggelse af kommunens brugeres adgange og rettigheder.	Inspiceret proceduren for registrering og nedlæggelse af brugere. Stikprøvevist påset, at processen for oprettelse og nedlæggelse af IT-Forsyningens brugere er fulgt i erklæringsperioden.	Ingen afvigelser konstateret.
9.2.2 Tildeling af brugeradgang Adgang- og brugerrettigheder tildeles på baggrund af sag i ServiceDesk-system fra ansvarlig leder.	Ejerkommunerne har selv ansvaret for at kommunikere til IT-Forsyningen i forbindelse med oprettelse, ændringer samt nedlæggelse af kommunens brugeres adgange og rettigheder.	Stikprøvevist påset, at adgang og brugerrettigheder for IT-Forsyningens brugere tildeles med afsæt i en formel godkendelse fra ansvarlig leder.	Ingen afvigelser konstateret.
9.2.3 Styring af privilegerede adgangsrettigheder Udvidede rettigheder tildeles på baggrund af en sag i ServiceDesk-systemet og kun med afsæt i et ledelsesgodkendt arbejdsbetinget behov.	Ejerkommunerne har selv ansvaret for at kommunikere til IT-Forsyningen i forbindelse med oprettelse, ændringer samt nedlæggelse af kommunens brugeres adgange og rettigheder.	Inspiceret proceduren vedrørende tildeling og anvendelse af administrative privilegier. Stikprøvevist påset, at tildeling af udvidede rettigheder for IT-Forsyningens brugere sker med afsæt i et ledelsesgodkendt arbejdsbetinget behov.	Ingen afvigelser konstateret.
9.2.4 Styring af hemmelig autentifikationsinformation om brugere Password og brugernavn kommunikeres aldrig til brugerne samlet og ukrypteret.	Ingen.	Forespurgt, hvorledes password og brugernavn kommunikeres til nye medarbejdere med henblik på at konstatere, at disse ikke kommunikeres samlet og ukrypteret.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
9.2.5 Gennemgang af brugeradgangs-rettigheder IT-Forsyningen foretager som minimum én gang årligt en revurdering af egne brugere, herunder deres adgang og rettigheder.	Ejerkommunerne har selv ansvaret for at etablere kontroller, der sikrer, at der periodisk følges op på egne brugere og de tildelte rettigheder. IT-Forsyningen leverer på bestilling udtræk over oprettede, aktive og inaktive brugere i AD.	Inspiceret proceduren vedrørende ledelsens periodiske gennemgang af brugernes adgange og adgangsrettigheder. Stikprøvevist påset, at gennemgangen har fundet sted i erklæringsperioden.	Ingen afvigelser konstateret.
9.2.6 Inddragelse eller justering af adgangsrettigheder Inddragelse eller justering af brugeres adgangsrettigheder sker rettidigt i systemer og platforme på baggrund af sag i ServiceDesk-system fra ansvarlig leder.	Ejerkommunerne har selv ansvaret for at kommunikere til IT-Forsyningen i forbindelse med nedlæggelse af kommunens brugere.	Inspiceret proceduren vedrørende inddragelse eller justering af adgangsrettigheder. Stikprøvevist påset, at det i forbindelse med ændringer i ansættelsesforholdet sikres, at brugernes adgange og rettigheder ændres, hvis nødvendigt.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.9 – Adgangsstyring			
A.9.4 – Styring af system- og applikationsadgang			
Formål: At forhindre uautoriseret adgang til systemer og applikationer.			
9.4.1 Begrænset adgang til informationer Der er udarbejdet en passwordpolitik, som stiller følgende krav til passwords: • Kompleksitet er slået til • Minimum otte karakterer • Skal skiftes hver 90. dag • Kan først skiftes efter en dag • 24 passwords bliver husket. • Låses efter 3 mislykkede log-in forsøg	Det er ejerkommunernes ansvar at kommunikere konfigurationskrav til opsætning af password på egne servere og databaser med henblik på at sikre, at dette opfylder ejerkommunens egne krav hertil.	Inspiceret Domain Controller-serveren hos IT-Forsyningen med henblik på at konstatere, om password er implementeret i overensstemmelse med passwordpolitikken. Inspiceret Domain Controller-serveren hos ejerkommunerne med henblik på at konstatere, om passwords er implementeret i overensstemmelse med kommunernes krav herfor.	Ingen afvigelser konstateret.
9.4.2 Procedurer for sikker log-on Adgang til systemer og data er forsvarligt beskyttet med afsæt i ovenstående passwordpolitik.	Ingen.	Inspiceret Domain Controller-serveren hos IT-Forsyningen med henblik på at konstatere, at der er opsat tvungne krav til passwords på IT-Forsyningens miljøer. Inspiceret Domain Controller-serveren hos ejerkommunerne med henblik på at konstatere, om der er opsat tvungne krav til passwords på ejerkommunernes miljøer i henhold til ejerkommunernes passwordpolitikker.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
9.4.3 System for administration af adgangskoder Passwords skal altid skiftes efter første login. Førstegangs-password er komplekst for at undgå, at dette kan regnes ud og udnyttes. Password til serviceprofiler, systembrugere samt standardbrugere opbevares beskyttet, og kun medarbejdere med et arbejdsbetinget behov har adgang.	Ingen.	Inspiceret opbevaring af password til serviceprofiler, systembrugere og standardbrugere med henblik på at konstatere, om passwords opbevares forsvarligt, samt om kun medarbejdere med et arbejdsbetinget behov har adgang hertil.	Ingen afvigelser konstateret.
9.4.4 Brug af privilegerede systemprogrammer Der anvendes ikke systemprogrammer, som kan omgå den logiske sikkerhed i systemer og platforme.	Ingen.	Forespurgt, hvorvidt der i IT-Forsyningen anvendes systemprogrammer, som kan omgå den logiske sikkerhed i systemer og platforme.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.11 – Fysisk perimetersikring			
A.11.1 – Sikre områder			
Formål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.			
11.1.1 Fysisk perimetersikring Adgang til datacentre i Ballerup og Allerød er sikret af elektroniske adgangskortlæsere, som er forbundet med centralt adgangskontrolsystem.	Ingen.	Inspiceret datacentrene -og perimetersikkerheden (bygninger, lokaler mv.) for Allerød og Ballerup med henblik på at konstatere, om de er sikret imod uautoriseret fysisk adgang og indtrængen.	Ingen afvigelser konstateret.
11.1.2 Fysisk adgangskontrol Tildeling af adgange for IT-Forsyningens medarbejdere sker efter godkendelse IT-Forsyningens ledelse.	Eftersom ejerkommunerne varetager oprettelse og nedlæggelse af adgange til datacentrene, er de ansvarlige for adgangene i dagligdagen, herunder sikring af at der ikke tildeles adgange, som IT-Forsyningen ikke bliver gjort bekendt med.	Inspiceret, at særligt sensitive områder er sikret med passende adgangskontroller. Stikprøvevist påset, at adgange til datacentre kun tildeles på baggrund af en godkendt request samt et arbejdsbetinget behov. Stikprøvevist inspiceret IT-Forsyningens egenkontrol af adgangskort og tildelte adgange med henblik på at vurdere effektiviteten af denne.	Ingen afvigelser konstateret.
11.1.3 Sikring af kontorer, lokaler og faciliteter Adgang til kontorer og lokaler hos IT-Forsyningen er sikret med nøgle og elektroniske adgangskortlæsere.	Ejerkommunerne har selv ansvaret for at etablere kontroller med henblik på at sikre egne kontorer og lokaler.	Inspiceret, at kontorer og lokaler hos IT-Forsyningen er sikret med nøgle og elektroniske adgangskortlæsere.	Ingen afvigelser konstateret.
11.1.4 Beskyttelse mod eksterne og miljømæssige trusler Datacentrene i Ballerup og Allerød er udstyret med nødstrøm, hævede gulve og vandføling.	Ingen.	Inspiceret datacentrene i Allerød og Ballerup med henblik på at konstatere, om der er implementeret betryggende beskyttelse mod eksterne og miljømæssige trusler i form af: • Klimaovervågning • Brandovervågning • Nødstrøm.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.11 – Fysisk perimetersikring			
A.11.2 – Udstyr			
Formål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.			
11.2.1 Placering og beskyttelse af udstyr Datacentrene i Ballerup og Allerød er placeret og indrettet således, at risikoen for miljøtrusler og farer samt muligheden for uautoriseret adgang nedsættes	Ingen.	Inspiceret datacentrene i Allerød og Ballerup med henblik på at konstatere tilstedeværelse af forebyggelsessystemer, herunder: • Hævede gulve • Sikring mod fugt • Vandføling • Brandslukningssystem • Nødstrøm.	Ingen afvigelser konstateret.
11.2.2 Understøttende forsyninger (forsyningssikkerhed) Datacentrene i Ballerup og Allerød er sikret med UPS-anlæg, der træder i kraft ved strømudfald på el-nettet. Det primære datacenter i Ballerup er endvidere beskyttet med generator, der kan sikre fortsat drift ved strømudfald.	Ingen.	Inspiceret datacentrene i Allerød og Ballerup med henblik på at konstatere, at der er etableret dubleret fremføring af strøm og nødstrøm i form af UPS samt dieselgenerator med tilstrækkelig kapacitet. Inspiceret servicerapporterne for Allerød og Ballerup kommune med henblik på at konstatere, at der udføres løbende eftersyn af: • UPS • Brandsikring • Køling • Dieselgenerator i Ballerup.	Ingen afvigelser konstateret.
11.2.3 Sikring af kabler Kabler til elektricitet og telekommunikation er placeret forsvarligt og beskyttet mod indgreb.	Ingen.	Inspiceret datacentrene for Allerød og Ballerup med henblik på at konstatere, at kabler til elektricitet og telekommunikation er placeret forsvarligt og beskyttet mod indgreb.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
11.2.7 Sikker bortskaffelse eller genbrug af udstyr Der er indgået aftale i forbindelse med destruktion eller genanvendelse af hardware, som sikrer, at følsomme data slettes fra udstyr inden bortskaffelse.	Ingen.	Inspiceret indgået aftale med ekstern part i forbindelse med destruktion eller genanvendelse af hardware. Inspiceret dokumentation for, at der er gennemført sikker bortskaffelse af udstyr i 2021.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.12 – Driftssikkerhed			
A.12.1 – Driftsprocedurer og ansvarsområder			
Formål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter			
12.1.1 Dokumenterede driftsprocedurer IT-Forsyningen har udarbejdet formelle driftsprocedurer for så vidt angår den daglige drift, herunder backup, patch management og change management. Disse vedligeholdes løbende.	Ingen.	Inspiceret et udvalg af driftsdokumentationen med det formål at sikre, at den er opdateret og tilgængeligt for de medarbejdere, der har behov for driftsdokumentationen. Inspiceret anvendelse af værktøjer til brug for overvågning af servere og netværk. Stikprøvevist påset, at IT-Forsyningens miljøer er underlagt overvågning. Inspiceret at ejerkommunerne har fremsendt klassifikation af systemer til IT-Forsyningen, og stikprøvevist påset, at ejerkommunernes servere og netværk er underlagt overvågning, jf. Klassifikationen. Inspiceret, at der er etableret 24/7/365-vagtordning, samt at systemet er sat op til at alarmere vagten ved nedbrud eller incidents. Stikprøvevist inspiceret håndteringen af incidents, med henblik på at konstatere, at der foretages opfølgning på incidents.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
12.1.2 Ændringsstyring IT-Forsyningen har udarbejdet en formel change management-procedure, som foreskriver, at der i forbindelse med ændringer foretages stillingtagen til: • Formål • Test • Fallback • Timing	IT-Forsyningen foretager ikke ændringer til ejerkommunernes fagsystemer.	Inspiceret proceduren vedrørende ændringer til servere, databaser og netværk. Stikprøvevist inspiceret, at ændringer foretaget på platforme, databaser og netværksudstyr er håndteret i overensstemmelse med change management-proceduren.	Ingen afvigelser konstateret.
12.1.4 Adskillelse af udviklings-, test- og driftsmiljøer IT-Forsyningen har udpeget specifikke servere af ukritisk karakter, som anvendes til test i forbindelse med patching af IT-Forsyningens egne servere samt ejerkommunens servere.	Ejerkommunerne har selv ansvar for at sikre den logiske adskillelse mellem udviklings-, test- og driftsmiljøer for deres fagsystemer.	Stikprøvevist inspiceret, at der er udpeget specifikke servere af ukritisk karakter, som anvendes til test i forbindelse med patching af IT-Forsyningens egne servere samt ejerkommunens servere.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.12 – Driftssikkerhed			
A.12.2 – Beskyttelse mod malware			
Formål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware			
12.2.1 Kontroller mod malware Der er etableret antivirussystem på alle PC'er samt på alle servere, som er konfigureret til automatisk opdatering. Webtrafik-filtrering er etableret for IT-Forsyningen og ejerkommunerne. Der foretages virus-, malware- og spamscanning af alle indgående og udgående e-mails.	Ballerup Kommune har selv driftsansvaret for egen mailløsning, herunder også ansvaret for scanning af e-mails for virus.	Stikprøvevist inspiceret, at servere såvel som arbejdsstationer er beskyttet med antivirus-software, samt stikprøvevist inspiceret konfigurationen med henblik på at sikre, at løsningen er opdateret. Stikprøvevist inspiceret, at webtrafik-filtrering er etableret for IT-Forsyningen og ejerkommunerne, samt stikprøvevist påset, at indgående og udgående e-mails scannes for virus og malware.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.12 – Driftssikkerhed			
A.12.3 – Backup			
Formål: At beskytte mod tab af data			
12.3.1 Backup af information IT-Forsyningen og ejerkommunerne har fastlagt en strategi for backup, som indgår i IT-Forsyningens servicekatalog. Der anvendes Veeam til backup af servere. Der tages daglig incremental- og ugentlig fuld backup. Retention time er minimum 14 dage. Der foretages en daglig dokumenteret efterkontrol af backup.	IT-Forsyningen tager backup af ejerkommunernes data, jf. aftale. Det er ejerkommunernes ansvar at kommunikere backupkrav til IT-Forsyningen, samt sørge for at der tages backup af fagsystemer i henhold til gældende lovgivning.	Stikprøvevist inspiceret proceduren vedrørende backup af systemer og data, herunder opsætning i Veeam backup-værktøjet dækkende for både ejerkommunerne samt IT-Forsyningen internt. Inspiceret procedure vedrørende test af gendannelse af systemer og data fra backup. Stikprøvevist inspiceret, at der gennemføres opfølgning på fejlede backupjobs.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.12 – Driftssikkerhed			
A.12.4 – Logning og overvågning			
Formål: At registrere hændelser og tilvejebringe bevis			
12.4.1 Hændelseslogning Der er etableret hændelseslogning af brugeraktivitet, undtagelser og fejl på servere og databaser. Logning gennemgås reaktivt ved behov og ved mistanke om uregelmæssighed.	Det er ejerkommunernes ansvar at kommunikere konfigurationskrav til opsætning af logning på egne servere og databaser, med henblik på at sikre, at dette opfylder ejerkommunens egne krav hertil samt relevante logkrav. Ejerkommunerne er selv ansvarlige for opsætning af logning i fagsystemerne samt periodisk gennemgang heraf.	Inspiceret procedurer vedrørende logning hos IT-Forsyningen. Inspiceret logopsætningen på IT-Forsyningens servere og databaser for at konstatere, om auditlogning var aktiveret i overensstemmelse med proceduren. Inspiceret aftaler med ejerkommunerne vedrørende opsætning, udførelse, registrering og opbevaring af audit-logning i forbindelse med hændelseslogning. Stikprøvevist kontrolleret logopsætning på ejerkommunernes servere og databaser for at konstatere, om auditlogning var aktiveret i henhold til aftaler og procedurer. Forespurgt til procedure vedrørende gennemgang af logge.	Ingen afvigelser konstateret.
12.4.2 Beskyttelse af logoplysninger Logoplysninger opbevares på servere, således at det kræver administratorrettigheder at tilgå logge.	Ingen.	Stikprøvevist kontrolleret, at logoplysninger opbevares på servere, således at det kræver administratorrettigheder at tilgå logge.	Ingen afvigelser konstateret.
12.4.3 Administrator- og operatørlog Aktiviteter, der er udført af systemadministratorer, logges. Logning gennemgås reaktivt efter behov og ved mistanke om uregelmæssighed.	Ingen.	Stikprøvevist inspiceret, at aktiviteter, der er udført af systemadministratorer, logges. Forespurgt til procedure vedrørende gennemgang af logge.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.12 – Driftssikkerhed			
A.12.5 – Styring af driftssoftware			
Formål: At sikre integriteten af driftssystemer			
12.5.1 Softwareinstallation på drifts-software Der er udarbejdet formelle patch manage-ment-procedurer, som omfatter IT-Forsy-ningen og ejerkommunernes servere og da-tabaser. Der gennemføres ved behov – højst én gang månedligt i aftalt servicevindue – in-stallation af patches på samtlige Windows-systemer. Kritiske og akutte ændringer kan foretages om nødvendigt udenfor aftalte service-vin-duer mod foregående aftale med kommu-nerne.	Ingen.	Inspiceret patch management procedurer. Stikprøvevist inspiceret at patching af ser-vere og databaser foretages i overensstem-melse med proceduren. Forespurgt, om der er foretaget kritiske og akutte ændringer uden for aftalte service-vin-duer.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.12 – Driftssikkerhed			
A.12.6 – Styring af driftssoftware			
Formål: At forhindre, at tekniske sårbarheder udnyttes.			
12.6.1 Styring af tekniske sårbarheder Patches til servere og databaser vurderes månedligt for relevans og kritikalitet. Patches til netværksenheder vurderes i forbindelse med de frigives for relevans og kritikalitet.	Ingen.	Stikprøvevist inspiceret, at der indsamles rettidig information om tekniske sårbarheder i anvendte netværksenheder, samt at disse evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.13 – Kommunikationssikkerhed			
A.13.1 – Styring af netværkssikkerhed			
Formål: At sikre beskyttelse af informationer i netværk og af understøttende informationshandlingsfaciliteter			
13.1.1 Netværksstyring Netværk overvåges løbende, med henblik på at sikre forsvarlig beskyttelse af informationer i systemer og applikationer. Implementering af nye kritiske komponenter samt ændring af eksisterende dokumenteres og godkendes via change management proces forud for udførsel.	Ingen.	Inspiceret procedure vedrørende styring og kontrol af netværk. Inspiceret anvendelse af værktøjer til brug for overvågning af servere og netværk. Stikprøvevist inspiceret, at ændringer, foretaget på platforme, databaser og netværksudstyr er håndteret i overensstemmelse med Change Management proceduren. Inspiceret, at IT-Forsyningen har implementeret kontroller, hvor IT-Forsyningen periodisk foretager netværks- og sårbarhedsscanninger, med henblik på at konstatere, at netværk er opsat og styret betryggende.	Ingen afvigelser konstateret.
13.1.2 Sikring af netværkstjenester Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester indgår i aftaler om netværkstjenester.	Ingen.	Inspiceret procedure vedrørende styring og kontrol af netværk. Stikprøvevist inspiceret, at IT-Forsyningen har identificeret sikkerhedstiltag, serviceniveauer og styringskrav til alle netværkstjenester og sikret, at disse indgår i aftaler om netværkstjenester.	Ingen afvigelser konstateret.
13.1.3 Opdeling af netværk Der er sikret fuld segmentering mellem ejerkommunernes netværk samt IT-Forsyningens netværk via firewalls.	Ingen.	Inspiceret procedure vedrørende oprettelse og styring af netværk for ejerkommunerne, herunder firewall og adskillelse af netværk. Stikprøvevist inspiceret netværksdiagrammer, med henblik på at konstatere, at der er etableret betryggende segmentering mellem ejerkommunernes samt IT-Forsyningens netværk.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.13 – Kommunikationssikkerhed			
A.13.2 – Informationsoverførsel			
Formål: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet			
13.2.1 Politikker og procedurer for informationsoverførsel Personfølsomme oplysninger eller forretningskritisk information sendes ikke ukrypteret via åbne netværk.	Ejerkommunerne har selv ansvaret for at udarbejde politikker og procedurer for informationsoverførsel med afsæt i egne sikkerhedskrav samt relevante lovkrav.	Inspiceret procedure vedrørende informationsoverførsel. Forespurgt, hvorledes IT-Forsyningen sikrer, at personfølsomme oplysninger eller forretningskritisk information ikke sendes ukrypteret via åbne netværk.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.15 – Leverandørforhold			
A.15.1 – Informationssikkerhed			
Formål: At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til			
15.1.1 Informationssikkerhedspolitik for leverandørforhold Eksterne leverandører, som skal have adgang til IT-Forsyningens aktiver, skal efterleve gældende informationssikkerhedspolitik for IT-Forsyningen. Eksterne konsulenter skal underskrive fortrolighedserklæring.	Ingen.	Stikprøvevist påset, at eksterne leverandører efterlever gældende informationspolitik for IT-Forsyningen. Stikprøvevist påset, at eksterne konsulenter underskriver en fortrolighedserklæring forud for, at de tildeles adgang til systemer og data.	Ingen afvigelser konstateret.
15.1.2 Håndtering af sikkerhed i leverandøraftaler Leverandøraftaler evalueres løbende, for at sikre, at disse afspejler informationssikkerhedsniveauet i IT-Forsyningen.	Ingen.	Forespurgt omkring, hvorledes det sikres, at leverandøraftaler evalueres løbende. Stikprøvevist inspiceret, at leverandøraftaler evalueres løbende, med henblik på at konstatere, om det sikres, at de afspejler informationssikkerhedsniveauet i IT-Forsyningen.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.16 – Styring af informationssikkerhed			
A.16.1 – Styring af informationssikkerhedshændelser og forbedringer			
Formål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og -svagheder.			
16.1.1 Ansvar og procedurer Der er udarbejdet procedure i forbindelse med informationssikkerhedshændelser, indeholdende stillingtagen til ansvarsplacering, rapportering, procedurer, diskretion og håndtering.	Ingen.	Inspiceret procedurer for rapportering af informationssikkerhedshændelser, med henblik på at konstatere, om denne indeholder stillingtagen til ansvarsplacering, rapportering, procedurer, diskretion og håndtering.	Ingen afvigelser konstateret.
16.1.2 Rapportering af informationssikkerhedshændelser Medarbejdere er gjort bekendte med procedurerne vedrørende rapportering af informationssikkerhedshændelser. Sikkerhedshændelser opdages via monitorering eller brugernes indmeldinger og håndteres af udvalgte medlemmer af IT-Forsyningens personale, og håndbæres umiddelbart efter opdagelse er sket. Sikkerhedshændelser rapporteres til leder.	Ejerkommunerne er ansvarlige for rapportering af alle problemer, der kan have indflydelse på driften af kommunens systemer og applikationer.	Stikprøvevist inspiceret, at informationssikkerhedshændelser rapporteres til ledelsen og håndtering af disse foretages betryggende.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.17 – Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring			
A.17.1 – Informationssikkerhedskontinuitet			
Formål: Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.			
17.1.1 Planlægning af informationssikkerhedskontinuitet Hændelser, der kan forårsage afbrydelser af forretningsprocesser er identificeret, og der er udarbejdet en beredskabsplan for IT-Forsyningen med afsæt heri.	Ingen.	Inspiceret it-beredskabsplanen med henblik på at konstatere, om it-beredskabsplanen tager afsæt i en risikovurdering.	Ingen afvigelser konstateret.
17.1.2 Implementering af informationssikkerhedskontinuitet Der er udarbejdet og opretholdt en proces til beredskabsstyring hos IT-Forsyningen, som behandler de krav til informationssikkerhed, der er nødvendige for virksomhedens fortsatte drift.	Ingen.	Forespurgt, om der er udarbejdet og implementeret en it-beredskabsplan, der omfatter alle it-systemer. Forespurgt om procedurer om beredskabsstyring og opdatering heraf med afsæt i en risikovurdering.	Ingen afvigelser konstateret.
17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten Beredskabsplanen afprøves og opdateres regelmæssigt for at sikre, at den er tidssvarende og effektiv.	Ingen.	Inspiceret it-beredskabsplanen med henblik på at konstatere, om it-beredskabsplanen indeholder krav om periodisk revurdering for at sikre, at den til enhver tid afspejler behovet for reetablering af it-systemer. Forespurgt om procedurer for opdatering af beredskabsplanen på baggrund af periodisk test heraf. Inspiceret testplan for test af it-beredskabsplanen, herunder om der foreligger resultat og rapportering til ledelsen af den afholdte test.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.17 – Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring			
A.17.2 – Redundans			
Formål: At sikre tilgængelighed af informationsbehandlingsfaciliteter			
17.2.1 Tilgængelighed af informations-behandlingsfaciliteter Primært datacenter er i Ballerup, hvorfra drift foretages, og sekundært datacenter er i Værløse, hvor backup af data opbevares, hvorved der er sikret adskillelse mellem informationsbehandlingsfaciliteter.	Ingen.	Inspiceret datacentrene i Allerød og Ballerup, med henblik på at konstatere, at der er sikret adskillelse mellem informationsbehandlingsfaciliteter, samt om datacentrene er beskyttet mod ekstreme fysiske forhold vedrørende brand, vand og varme.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.18 – Overensstemmelse			
A.18.1 – Overensstemmelse med lov- og kontraktkrav			
Formål: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet			
18.1.1 Identifikation af gældende lovgivning og kontraktkrav IT-Forsyningen tilstræber at overholde alle relevante bestemmelser, regulering og kontraktlige forpligtelser. Juridisk bistand rekvireres om fornødent fra ejerkommunerne.	Ingen.	Forespurgt, hvorledes IT-Forsyningen sikrer overholdelse af lov- og kontraktkrav. Forespurgt, om der i revisionsperioden har været behov for at rekvirere juridisk bistand fra ejerkommunerne.	Ingen afvigelser konstateret.

Nr.	Kommunernes ansvar	Udførte test	Resultater af test
A.18 – Overensstemmelse			
A.18.2 – Gennemgang af informationssikkerhed			
Formål: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet			
18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder Lederne i IT-Forsyningen sikrer overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder samt rapporterer uoverensstemmelse.	Ingen.	Forespurgt, hvorledes lederne i IT-Forsyningen sikrer overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder. Stikprøvevist inspiceret, om identificerede uoverensstemmelser rapporteres.	Ingen afvigelser konstateret.
18.2.3 Undersøgelse af teknisk overensstemmelse Der foretages periodisk undersøgelse af informationssystemerne i IT-Forsyningen for at sikre overensstemmelse med IT-Forsyningens informationssikkerhedspolitikker og –standarder.	Det er ejerkommunernes ansvar at kommunikere konfigurationskrav til opsætning af egne servere og databaser, med henblik på at sikre, at den tekniske sikkerhed i disse konfigureres i overensstemmelse med ejerkommunernes informationssikkerhedspolitikker og –standarder.	Forespurgt, hvorledes IT-Forsyningen sikrer, at der er overensstemmelse mellem informationssystemerne og IT-Forsyningens informationssikkerhedspolitikker og –standarder. Stikprøvevist inspiceret, om der periodisk foretages undersøgelse af informationssystemerne i IT-Forsyningen.	Ingen afvigelser konstateret.

5. Supplerende information fra IT-Forsyningen

IT-Forsyningen har igangsat en række initiativer med henblik på at fastholde og øge sikkerhedsniveauet.

- IT-Forsyningen har sammen med ejerkommunerne i sin ejerstrategi besluttet at etablere et særskilt fokus på sikkerhed og igangsætte indsatser, der skal hæve fastholde og hæve sikkerhedsniveauet yderligere. Udvælgelse og prioritering af indsatserne sker i samarbejde med ejerkommunerne.