



## Curanet A/S

### **ISAE 3402 type 2 erklæring om generelle it-kontroller relateret til hostingydelser.**

Erklæringen omfatter perioden fra 01.01.2019 til 31.12.2019

## **Indholdsfortegnelse**

|   | <b>Side</b> |
|---|-------------|
| 1. Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet | 1           |
| 2. Serviceleverandørs udtalelse   | 4           |
| 3. Serviceleverandørs systembeskrivelse   | 6           |
| 4. Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf  | 14          |

## **1. Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet**

Til: ledelsen hos Curanet A/S, Curanet A/S' kunder og deres revisorer

### **Omfang**

Vi har fået til opgave at afgive erklæring om Curanet A/S' (herefter "Curanet") beskrivelse i afsnit 3 for Curanets hostingydelser omfattende udformning, implementering og funktionalitet af kontroller anført i beskrivelsen i hele perioden fra 01.01.2019 til 31.12.2019, og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Erklæringen omfatter de fælles generelle it-kontroller, som varetages af Curanet i forbindelse med levering af generelle hostingydelser. Der kan således være indgået eventuelle særlige aftaleforhold mellem Curanet og kunden, som ligger uden for de generelle standardydelser, hvorfor disse ikke er omfattet af denne erklæring.

Curanets systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos anvendte serviceunderleverandører, og denne erklæring omfatter således ikke kontroltest af kontroller hos serviceunderleverandører. Curanet benytter følgende underleverandører til fysisk sikring af produktionsmiljøer og ekstern opbevaring af backup:

- Nianet A/S / Fuzion A/S:
  - Housing
  - Fysisk sikring af produktionsmiljø
- GlobalConnect A/S:
  - Housing
  - Fysisk sikring af produktionsmiljø
  - Ekstern opbevaring af backup (indtil oktober)
- Cibicom A/S (fra oktober 2019):
  - Housing
  - Fysisk sikring af produktionsmiljø
  - Ekstern opbevaring af backup.

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

### **Curanets ansvar**

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

### **Vores uafhængighed og kvalitetsstyring**

Vi har overholdt kravene til uafhængighed i IESBA's Ethiske 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 til 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 Curanets 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 kontrollerens 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 og 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**

Curanets 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 Curanets hostingydelser og kontrolmiljø, således som det var udformet og implementeret i hele perioden fra 01.01.2019 til 31.12.2019, 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 fra 01.01.2019 til 31.12.2019
- (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 fra 01.01.2019 til 31.12.2019.

#### **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 kunder, der har anvendt Curanets ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 17. marts 2020

**Deloitte**

Statsautoriseret Revisionspartnerselskab  
CVR-nr. 33 96 35 56



Thomas Kühn  
statsautoriseret revisor



Michael Bagger  
director, CISA

## 2. Serviceleverandørs udtalelse


Medfølgende beskrivelse er udarbejdet til brug for Curanet A/S' kunder 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 risiciene for væsentlig fejlinformation i kundernes regnskaber. Curanet A/S bekræfter, at

- a) den medfølgende beskrivelse i afsnit 3 giver en retvisende beskrivelse af de generelle kontroller i tilknytning til Curanet A/S' hostingydelser i hele perioden fra 01.01.2019 til 31.12.2019. 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 det 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 information 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 brugervirksomheder, 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 serviceleverandørens kontrolmiljø for drifts- og hostingydelser foretaget i perioden fra 01.01.2019 til 31.12.2019.
  - 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 fra 01.01.2019 til 31.12.2019. 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
  - iii. kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 01.01.2019 til 31.12.2019.

Skanderborg, den 17. marts 2020

Curanet A/S



Stefan Rosenlund  
Adm. direktør

### 3. Serviceleverandørs systembeskrivelse

#### 3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Curanets kunder og disses revisorer og for at opfylde kravene i revisionsstandard ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør".

Beskrivelsen er ligeledes udfærdiget med det formål at give information om de kontroller, der anvendes, i forhold til levering af hostingydelser og it-driftsydelser leveret af Curanet.

#### 3.2 Beskrivelse af Curanets ydelser

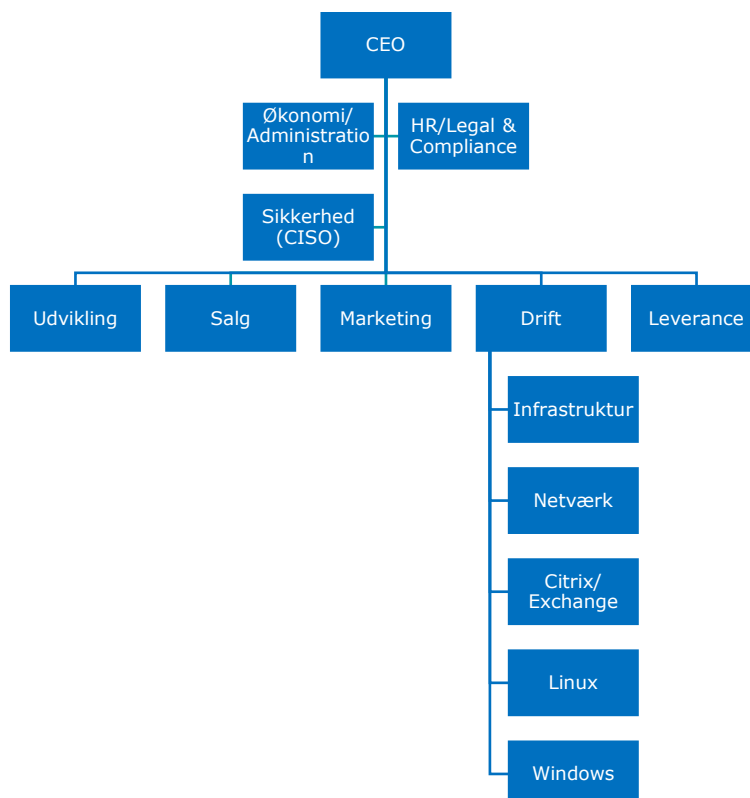
Curanet udvikler, administrerer og servicerer en vifte af professionelle hosting- og cloud-løsninger for en lang række virksomheder og organisationer i Danmark.

Curanet arbejder ud fra en stræben efter at levere løsninger, der kvalitets- og servicemæssigt differentierer sig fra størstedelen af det resterende hosting-marked. Med mange års erfaring på markedet har Curanet erfaret, at graden af kunders tilfredshed har direkte sammenhæng med niveauet af leverandørens service, tekniske kompetencer og kvaliteten af det hardware, som Curanets løsninger driftes på. Det er derfor i stor stil de værdier, vi baserer vores forretning på.

Fundamentet i forretningen er et moderne datacenter, som vi drifter med udgangspunkt i, at det skal kunne supportere stabilitet, sikkerhed og en hastighed, der kan imødekomme servicekrav fra kritiske og kvalitetsbevidste kunder. Med vores højt certificerede og fagligt erfarne medarbejdere kan vi støtte op om enhver type hosting-løsning – altid med kompetent rådgivning.

#### 3.3 Curanets organisation og sikkerhed

Ansvar og organisering i Curanet fremgår af nedenstående organisationsdiagram. Sikkerhedschefen (CISO) referer til den administrerende direktør (CEO).





Organisationens arbejde med sikkerhed styres og prioriteres af Sikkerhedsudvalget, som består af følgende medlemmer:

- CEO, Stefan Rosenlund
- CTO, Ole P. Jensen
- Chief Legal Officer, Bo Brandt Cramer
- CISO, Jakob Flink Schwartz.

### **3.4 Risikostyring hos Curanet**

Risikostyring gennemføres i Curanet på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering, der sigter mod udvalgte systemer. Input til denne vurdering indhentes fra alle relevante niveauer af organisationen. Processen faciliteres af ansvarlige og ledere, der udarbejder udkast til Curanets ledelse. Efter intern bearbejdning godkendes vurderingen af Curanets ledelse.

Risikostyringen tager højde for forhold, som er nødvendige for at kunne styre risici i forhold til leverancen til kunderne. Dette sker gennem it-ledelsens kendskab til typer af aftaler mellem Curanet og kunderne.

Curanet har som led i ISO 27001-certificeringen etableret en formaliseret risikostyring, som omfatter alle relevante processer i virksomheden, der anvendes i leverancen af hosting-ydelser. Der følges op på risikovurderingen minimum én gang årligt ved det årlige ledelsesreview af ISO 27001-arbejdet. Arbejdet med risici er dokumenteret i et dokument, hvori både impact og sandsynlighed er beskrevet sammen med den samlede vægtning af hver enkelt risiko og de dertil knyttede handlinger. Relevante handlinger i forhold til væsentlige risici besluttet altid i samarbejde med ledelsen.

### **3.5 Kontrolrammer, kontrolstruktur og kriterier for kontrolimplementering**

Curanets it-sikkerhedspolitik, etablerede processer og kontroller omfatter alle systemer og ydelser, der tilbydes kunderne. Det fortsatte arbejde med tilpasning og forbedring af Curanets sikringsforanstaltninger sker løbende i samarbejde med højt kvalificerede specialister.

Fastsættelse af kriterier for og omfang af kontrolimplementeringen hos Curanet er i 2019 sket ud fra ISO 27001-/27002-standarden. Med udgangspunkt i dette kontrolrammeverk er relevante kontrolområder og kontrolaktiviteter implementeret på de serviceydelser, der leveres af Curanet.

Følgende væsentlige kontrolområder indgår i det samlede kontrolmiljø:

- Informationssikkerhed
- Intern organisering af it-sikkerhed
- Fysisk sikkerhed
- Styring af kommunikation med kunder
- Backup
- Drift og overvågning
- Adgangskontrol og logisk sikkerhed
- Anskaffelse og vedligeholdelse af systemsoftware
- Beredskabsplan
- Styring af leverandørydelser

### **3.6 Etableret kontrolmiljø**

Hvert enkelt område er beskrevet i detaljer i de efterfølgende afsnit.

#### **3.6.1 Informationssikkerhed**

##### **Formål**

En ledelsesgodkendt it-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse og er kommunikeret ud til relevante medarbejdere i virksomheden.

### **Anvendte procedurer og kontroller**

Curanet identificerer og afdækker relevante it-risici på de etablerede serviceydelser til kunderne. Dette varetages gennem en løbende trussels- og risikovurdering hos Curanet, dels i forbindelse med alle udviklingsprojekter og ændringer i systemmiljøer, dels ved en årlig revurdering af risikoanalysen. Resultatet af den årlige revurdering forelægges ledelsen til godkendelse. Curanet stiller endvidere en række informationer til rådighed for hosting-kundernes revisorer til brug ved deres vurdering af Curanet som serviceleverandør. Ud over driftsrelaterede forhold kan Curanet også informere om sikkerhedsmæssige forhold, i det omfang kunderne efterspørger dette.

### **Tidspunkt for udførelse af kontrollen**

It-risikoanalysen og it-sikkerhedspolitikken revurderes mindst én gang årligt inden udførelse af it-revision og udarbejdelse af erklæring.

### **Hvem udfører kontrollen?**

Den årlige gennemgang udføres af Sikkerhedsudvalget.

### **Kontroldokumentation**

Der sker versionsstyring af it-sikkerhedspolitikken.

### **3.6.2 Intern organisering af it-sikkerhed**

Direktionen i Curanet, som i det daglige er de øverst ansvarlige for it-sikkerheden, sørger for, at der til stadighed er etableret procedurer og tilknyttet systemer, der understøtter overholdelse af den til enhver tid gældende it-sikkerhedspolitik. Sikkerhedsgruppen beskriver de overordnede målsætninger, og den driftsansvarlige er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollerbart ud fra en ressourcemæssig vurdering af omkostninger og risiko, ligesom de enkelte kontrolaktiviteter på de serviceområder, som tilbydes kunderne, skal være inden for rammerne af ISO 27001. Sikkerhedsudvalget består p.t. af følgende medlemmer:

- CEO, Stefan Rosenlund
- CTO, Ole P. Jensen
- Chief Legal Officer, Bo Brandt Cramer
- CISO, Jakob Flink Schwartz.

Gruppen mødes én gang årligt for at fastsætte og følge op på målsætninger i relation til it-sikkerheden.

### **3.6.3 Styling af kommunikation med kunder**

#### **3.6.3.1 Service Desk og Curanet-support**

##### **Formål**

Der udføres tilfredsstillende support for kunder, der kontakter Service Desk, herunder ydes den aftalte support i det aftalte tidsrum.

##### **Anvendte procedurer og kontroller**

Service Desks håndtering af de enkelte kunder er baseret på et sæt skriftlige procedurer på de områder, der er aftalt med kunden. Brugersupport sker via e-mail, telefon og eventuelle fjernstyringsværktøjer.

##### **Tidspunkt for udførelse af kontrollen**

Service Desk behandler indkommende sager fra kunder.

##### **Hvem udfører kontrollen?**

Kontroller udføres af Service Desk.

##### **Kontroldokumentation**

Dokumentation for henvendelser og udførelse af opgaver for kunderne sker i Curanets sagsstyringssystem.

### **3.6.3.2 Incident-håndtering**

#### **Formål**

Der gennemføres en betryggende standardiseret incident-håndtering(driftsudmelding) for at sikre rettidig og åben kommunikation omkring driftsproblemer.

#### **Anvendte procedurer og kontroller**

Curanet anvender et sagsstyringssystem til registrering og håndtering af incidents, og der noteres følgende i sagen:

- Fejl eller problemstilling
- Tidsstempling for, hvad tid der er noteret i sagen
- Prioritering af fejlen
- Ekstern kommunikation, der skal gennemføres til eventuelt berørte brands.

Driftsafdelingens ledelse er ansvarlig for at incident-håndtering gennemføres i overensstemmelse med ovenstående.

#### **Tidspunkt for udførelse af kontrollen**

Incident-håndtering sker hurtigst muligt efter registrering af fejl/problem.

#### **Hvem udfører kontrollen?**

Håndteringen af incidents udføres af Curanets driftsafdeling, men kan også initieres af andre afdelinger efter behov. Inden for normal arbejdstid udføres den af vagthavende teknikere.

#### **Kontroldokumentation**

Dokumentation for incidents og udførelse af incidents for kunderne sker i Curanets sagsstyringssystem.

### **3.6.4 Backup**

#### **Formål**

Data sikkerhedskopieres og opbevares, så de kan reetableres i overensstemmelse med gældende SLA-krav. Curanet kontrollerer, om backup udføres fejlfrit, og ved fejl i backup kontrolleres det, at der udføres en vurdering af fejl og sker opfølgning på eventuel fejlretning.

#### **Anvendte procedurer og kontroller**

Der er udarbejdet en beskrivelse af backupproceduren. Backupproceduren er en del af den daglige kørsel og er således automatiseret i backupsystemet. Manuelle rutiner i forbindelse med backup er beskrevet i driftsprocedurerne. I forbindelse med backup anvendes underleverandøren Cibicom A/S til opbevaring af daglige kopier. Processen omkring backup varetages af Curanet. Der er etableret kontroller, som sikrer, at backup foretages på struktureret vis.

Der er følgende backupcyklus:

- Dagligt: backup af nye eller ændrede data
- Ugentligt: fuld backup af alle data og systemmiljøer.

Backup opbevares, således at mindst én backup er fysisk placeret andetsteds end produktionsdata. Der foretages mindst én gang årligt en test af, at tilfældigt udvalgte servere kan genskabes på baggrund af backupdata, og herudover finder restore af data sted i forbindelse med henvendelse fra kunderne.

#### **Tidspunkt for udførelse af kontrollen**

Der er etableret automatisk backup, og der gennemføres restore-test minimum én gang årligt.

#### **Hvem udfører kontrollen?**

Driftsafdelingen forestår den daglige kontrol af backuplogge.

### **Kontroldokumentation**

Backup log opbevares i Curanets asset management-system.

### **3.6.5 Drift og overvågning**

#### **Formål**

At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

#### **Anvendte procedurer og kontroller**

Curanet har etableret et sæt skriftlige driftsprocedurer på alle væsentlige driftsaktiviteter, som er afstemt med Curanets krav og den tilhørende it-sikkerhedspolitik og dels med de generelle forretningsbetingelser. Driftsprocedurerne er udarbejdet af driftsafdelingen og omfatter den aftalte drift og overvågning af systemmiljøerne.

Konstaterede fejl i udførte kontroller og eventuelle fejl fra overvågningssystemet korrigeres hurtigst muligt. Curanet informerer løbende om omfanget af og konsekvenserne ved de konstaterede fejl. Afvikling af batchjobs logges automatisk, således at der kan foretages opfølgende kontrol. Servere overvåges ved hjælp af monitoreringssoftware.

Følgende funktionsområder har adgang til kundernes it-systemer: Service Desk-medarbejdere og driftsmedarbejdere.

#### **Tidspunkt for udførelse af kontrollen**

Overvågning og opfølgning udføres 24/7 eller i den primære driftstid ifølge SLA-aftalen med den enkelte kunde.

#### **Hvem udfører kontrollen?**

Kontroller udføres af Curanets driftsafdeling, og uden for normal arbejdstid udføres de af forvagten.

### **Kontroldokumentation**

Den automatiske overvågning dokumenteres i Curanets overvågningssystem.

### **3.6.6 Adgangskontrol og logisk sikkerhed**

#### **Formål**

Adgang til systemer, data og andre it-ressourcer administreres, vedligeholdes og overvåges i overensstemmelse med Curanets retningslinjer.

Adgangen deles op i tre områder:

- Kundernes medarbejdere
- Curanets medarbejdere
- Medarbejdere hos tredjeparter.

#### **Anvendte procedurer og kontroller**

Det er kundens ansvar at sikre en betryggende adgang til de enkelte systemmiljøer, herunder at autentificere eventuel adgang til tredjepartsleverandør. Curanet forestår den tekniske oprettelse ud fra kundernes anvisninger, men det er kundens ansvar at kontrollere, at Curanet har oprettet brugerne i henhold til anvisningerne.

For Curanets interne brugere er informationssikkerhedsmæssige roller og ansvarsområder fordelt pr. afdeling, og medarbejderne bliver gjort bekendt med deres ansvar ved tiltrædelse.

Rettigheder til interne brugere hos Curanet oprettes efter formel godkendelse. For interne medarbejdere er der udarbejdet formelle retningslinjer vedrørende sletning af brugere. Disse sikrer bl.a., at en fratrædt medarbejder ved arbejdsophør hos Curanet spærres for login. Der foretages ligeledes en årlig kontrol af validiteten af de oprettede brugerkonti på Curanets interne systemer.

Der er defineret specifikke krav til kodeordskvalitet med hensyn til længde, kompleksitet, udskiftningshyppighed, historik og logningsniveau.

Navngivningen og opsætningen af brugerkonti til medarbejdere på de interne domæner sker således, at disse brugerkonti til enhver tid vil være personhenførbare.

#### **Tidspunkt for udførelse af kontrollen**

Kontrollen vedrørende brugeroprettelser sker, hver gang Curanet har en intern ansættelse eller fratrædelse. Kontrollen vedrørende inaktive brugere og brugere med administrative rettigheder foregår årligt.

#### **Hvem udfører kontrollen?**

Driftsafdelingen hos Curanet har ansvaret for, at adgangsprocedurene bliver overholdt.

#### **Kontroldokumentation**

Dokumentation vedrørende Curanets medarbejdere gemmes i et relevant værktøj.

### **3.6.7 Anskaffelse og vedligeholdelse af systemsoftware**

#### **Formål**

Systemsoftware vedligeholdes og supporteres, og ledelsen sikrer, at ændringer eller nyanskaffelser sker i overensstemmelse med virksomhedens behov, og at ændringer testes og dokumenteres på tilfredsstillende vis.

#### **Anvendte procedurer og kontroller**

For Windows-servere, som Curanet har driftsansvaret for, indhentes fyldestgørende systemdokumentation efter behov. Curanet har fastsat procedurer for anskaffelse og opdatering af systemsoftware på Windows-plattformene.

Nye Windows-servere, der sættes i drift, er konfigureret i overensstemmelse med den aktuelle baseline, som er defineret i en række scripts. Denne baseline indeholder specifikke krav til kodeord og patchning. Ansvar for kontrol af, at konfigurationsbaselinen er blevet opsat på servere og opfølgning på logning, overgår til kunder ved idriftsættelse. Der foretages en årlig revurdering af konfigurationsbaselinen.

Til Windows- og Linux-plattformen hentes opdateringer, og de udrulles automatisk på serverne. Netværksudstyr opdateres efter behov, og der defineres fallback-planer, inden opdatering gennemføres.

Patch af ESXi sker manuelt efter vurdering heraf.

#### **Tidspunkt for udførelse af kontrollen**

Kontrollen for opdatering sker via WSUS (Windows) eller Package Manager (Linux).

#### **Hvem udfører kontrollen?**

Driftsafdelingen er ansvarlig for udførelse af opdateringer og kontrol heraf.

#### **Kontroldokumentation**

Ud over dokumentation i WSUS fremgår installerede patches af den enkelte server.

### **3.6.8 Beredskabsplan**

#### **Formål**

En plan for genoptagelse af systemmiljøer hos Curanet, efter en katastrofe er indtruffet.

#### **Anvendte procedurer og kontroller**

Curanet har etableret en beredskabsplan, som overordnet set fastsætter retningslinjer for, hvordan en katastrofesituation skal håndteres. Beredskabsplanen godkendes årligt af Curanets ledelse.

Beredskabsplanen indeholder beskrivelse af følgende områder:

- Information om beredskabsplanen
- Organisering og kontrakter
- Oversigt over infrastruktur og tolerancegrænser for afbrydelse af forretningsprocesser
- Reaktionsplan, herunder klassificering af en nødsituation og regler for eskalering
- Krisestyringsplan, herunder retningslinjer for:
  - Initiering af beredskab
  - Skades- og situationsvurdering
  - Fastlæggelse af handlinger
  - Implementering og logistik
- Nøddrift og reetableringsplan.

Beredskabsplanen revurderes løbende og mindst én gang årligt, og der gennemføres verificering af den etablerede backup gennem en restore-test. Der gennemføres ikke større reetableringsøvelser eller fuld reetablering af hele systemmiljøer.

#### **Tidspunkt for udførelse af kontrollen**

Beredskabsplanen gennemgås og risikovurderes mindst én gang årligt.

#### **Hvem udfører kontrollen?**

Sikkerhedsgruppen udfører den årlige gennemgang og tilpasning af beredskabsplanen.

#### **Kontroldokumentation**

Der sker versionsstyring af beredskabsplanen. Der foreligger dokumentation for handlinger foretaget i forbindelse med 'dry run' af beredskabsplan.

### **3.6.9 Styring af leverandørydelser**

#### **Formål**

At sikre, at eventuelle afvigende kontroller hos eksterne leverandører bliver mitigeret.

#### **Anvendte procedurer og kontroller**

Der foretages kontrol af revisionserklæringer fra leverandører, som sikrer, at disse bliver gennemgået periodisk, og at eventuelle afvigelser i kontroller hos leverandører bliver mitigeret hos Curanet, hvor dette er relevant.

#### **Tidspunkt for udførelse af kontrollen**

Årlig gennemgang af revisionserklæringer

#### **Hvem udfører kontrollen?**

Ledelsen

#### **Kontroldokumentation**

Oversigt over leverandørydelser og kontrollen heraf

### **3.7 Supplerende information om det etablerede kontrolmiljø og forhold, som skal iagttages af kunders revisorer (komplementerende kontroller)**

#### **Levering af serviceydelser**

Ovenstående systembeskrivelse af kontroller er baseret på Curanets standardbetingelser. Det bevirker, at indgåede kundaftaler, som på de leverede serviceydelser er forskellige fra Curanets standardbetingelser, ikke er omfattet af nærværende erklæring. Kunderne og deres revisorer bør vurdere, om denne erklæring kan anvendes i forbindelse med vurdering af de generelle it-kontroller hos Curanet i relation til

drifts- og hosting-ydelser leveret fra Curanet til kunden. Kunderne og deres revisorer bør endvidere selv afdække eventuelle andre risici, der vurderes som væsentlige.

### **Brugeradministration**

Curanet giver adgang og tildeler rettigheder i overensstemmelse med kundernes instrukser, i takt med at disse bliver indmeldt gennem Service Desk. Curanet er ikke ansvarlig for, at informationer om brugere er korrekte, og det er således kundernes eget ansvar at sikre, at adgange og rettigheder til systemer og applikationer tildeles i overensstemmelse med kundens egne forventninger til betryggende brugeradministration, herunder funktionsadskillelse og periodisk revurdering i de systemmiljøer, som hostes og driftes af Curanet. Såfremt det ønskes, kan kunden selv oprette brugere på de enkelte servere – kontroller relateret til denne proces er kundernes eget ansvar.

### **Konfiguration af logisk sikkerhed**

Curanet har konfigureret logisk sikkerhed på sin egen infrastruktur i forbindelse med levering af drifts- og hostingydelser til sine kunder. Etablering og konfigurering af logisk sikkerhed på kundernes egne miljøer er udelukkende kundens ansvar, ligesom det er kundernes ansvar at kontrollere, at disse sikkerhedskonfigurationer er i overensstemmelse med det ønskede sikkerhedsniveau.

### **Backup**

Det er kundens eget ansvar at sikre, at backup opsættes i henhold til kundens eget behov. Retablering af kundedata fra backupsystemer testes kun, når der er indgået en specifik aftale herom med kunden, eller såfremt Curanet modtager henvendelse fra kunden med et specifikt ønske herom. I henhold til Curanets procedurer herfor er det efterfølgende kundens ansvar at sikre, at gennemført restore kan anvendes efter hensigten i de respektive miljøer.

### **Beredskabsplanlægning**

Curanet har opsat generel beredskabsplanlægning, der omfatter Curanets egen infrastruktur. Kunderne bør derfor selvstændigt vurdere, hvorvidt det er nødvendigt at implementere yderligere procedurer eller nødplaner, herunder efterprøvelse heraf.

### **Efterlevelse af relevant lovgivning**

Curanet er ikke ansvarlig for applikationer, som afvikles på det hostede udstyr. Det er således kundernes ansvar, at der er etableret betryggende kontroller i applikationerne, herunder at disse understøtter efterlevelse af bogføringsloven, persondataloven, lov om finansiel virksomhed og/eller anden relevant lovgivning.

## 4 Serviceleverandørs kontrolmål, kontroller, test og resultatet heraf

### 4.1 Introduktion

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

Vores test af Curanets kontroller er begrænset til de kontrolmål og relaterede 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 Curanets kontroller muligvis ikke kompensere for sådanne svagheder.

Curanets systembeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos serviceunderleverandøren, og denne erklæring omfatter således ikke kontroltest af kontroller hos serviceunderleverandøren. Curanet benytter følgende underleverandører til fysisk sikring af produktionsmiljøer og ekstern opbevaring af backup:

- Nianet A/S / Fuzion A/S:
  - Housing
  - Fysisk sikring af produktionsmiljø
- GlobalConnect A/S:
  - Housing
  - Fysisk sikring af produktionsmiljø
  - Ekstern opbevaring af backup (indtil oktober)
- Cibicom A/S (fra oktober 2019):
  - Housing
  - Fysisk sikring af produktionsmiljø
  - Ekstern opbevaring af backup.

Kundernes egne revisorer bør gennem indhentning af revisionserklæringer fra underleverandørerne foretage en samlet vurdering af, om alle nødvendige kontroller er på plads i relation til kundens samlede kontrolmiljø.

### 4.2 Test af kontroller

De udførte test i forbindelse med fastlæggelse af kontrollers funktionalitet består af en eller flere af følgende metoder:

| Metode                     | Beskrivelse  |
|----------------------------|--|
| Forespørgsel               | Forespørgsel hos udvalgt personale hos Curanet   |
| Observation                | Observation af kontrollens udførelse   |
| Inspektion                 | Inspektion af dokumenter og rapporter, som indeholder angivelse af udførelse 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 perioden fra 01.01.2019 til 31.12.2019.

Vores test af kontrollernes funktionalitet var udformet til at dække et repræsentativt antal af transaktioner i perioden fra 01.01.2019 til 31.12.2019 for hver kontrol, jf. nedenfor, som er udformet til at opnå de specifikke kontrolmål.

#### **4.4 Kontrolmål, kontroller og resultater af test**

I nedenstående skema er de testede kontrolmål og kontroller anført, ligesom vi har beskrevet, hvilke revisions handlinger der er udført og resultatet af disse handlinger. I det omfang vi har konstateret væsentlige kontrolsvagheder, har vi anført dette.

#### 4.4.1 Informationssikkerhed

Kontrolmål: At give retningslinjer for at understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

|  | <b>Etableret kontrol hos Curanet</b>  | <b>Udførte revisionshandlinger</b>  | <b>Konklusion</b>   |
|--|---|---|---------------------|
| 4.4.1.1<br><i>Politikker for informationssikkerhed</i> | Der er udarbejdet en it-sikkerhedspolitik, som gennemgås periodisk og minimum én gang årligt.   | Deloitte har inspiceret den seneste udgave af it-sikkerhedspolitikken og konstateret, at den er opdateret i erklæringsperioden.<br><br>Deloitte har stikprøvevist inspiceret it-sikkerhedspolitikken underliggende politikker og ved forespørgsel hos nøglepersonale fået bekræftet, at disse er gældende.<br><br>Deloitte har ved inspektion påset, at sikkerhedspolitikken er godkendt af ledelsen. | Ingen bemærkninger. |
| 4.4.1.2<br><i>It-risikoanalyse</i>                     | Curanet har udarbejdet en it-risikoanalyse, som dækker kritisk infrastruktur, der anvendes i den daglige drift.<br><br>Der gennemføres årligt en revurdering af, om forhold vedrørende risiko og trusler fortsat er gældende, eller om der er behov for at ændre i it-risikoanalysen. | Deloitte har inspiceret it-risikoanalysen og konstateret, at den er opdateret i erklæringsperioden.<br><br>Deloitte har ved inspektion påset, at it-risikoanalysen er godkendt af ledelsen.   | Ingen bemærkninger. |

#### 4.4.2 Intern organisering af it-sikkerhed

Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

|   | <b>Etableret kontrol hos Curanet</b>  | <b>Udførte revisionshandlinger</b>  | <b>Konklusion</b>   |
|---|---|---|---------------------|
| 4.4.2.1<br><i>It-sikkerhedsorganisation</i> | It-sikkerhedsmæssige roller og ansvarsområder er fordelt, og medarbejderne er bekendt med deres arbejdsopgaver og funktioner. | Deloitte har inspiceret en oversigt over roller i organisationen og konstateret, at den indeholder overordnede oplysninger om, hvem der har hvilke ansvarsområder i organisationen.<br><br>Deloitte har for en stikprøve af medarbejdere forespurgt, om de er bekendt med deres rolle og arbejdsopgaver | Ingen bemærkninger. |

#### 4.4.3 Styring af kommunikation med kunder

Kontrolmål: Der udføres tilfredsstillende support for kunder, der kontakter Service Desk, og der gennemføres en betryggende standardiseret incident-håndtering (driftsudmelding) for at sikre rettidig og åben kommunikation omkring driftsproblemer.

|   | <b>Etableret kontrol hos Curanet</b>   | <b>Udførte revisionshandlinger</b>  | <b>Konklusion</b>   |
|---|--|---|---|
| 4.4.3.1<br><i>Incident-håndtering</i>     | <p>Incidents registreres i sagsstyringssystemet. Dokumentation for incidents og udførelse af incidents for kunderne sker i Curanets sagsstyringssystem.</p> <p>Driftsafdelingens ledelse er ansvarlig for at incident-håndtering gennemføres i overensstemmelse med ovenstående.</p> | <p>Deloitte har stikprøvevist inspiceret registrerede incidents og verificeret, om incidents indeholder krævede oplysninger, og om incidents er lukkede.</p> <p>Deloitte har forespurgt nøglepersonale om, hvordan der sker opfølgning på sagerne for at sikre, at alle sager bliver behandlet korrekt.</p> | <p>Vi har konstateret for 2 stikprøver, at hændelser ved en manuel fejl er kategoriseret som incidents, men burde være kategoriseret som changes, der vedrører planlagt driftsarbejde</p> <p>Ingen yderligere bemærkninger.</p> |
| 4.4.3.2<br><i>Henvendelser fra kunder</i> | <p>Dokumentation for henvendelser og udførelse af opgaver for kunderne sker i Curanets sagsstyringssystem.</p>   | <p>Deloitte har stikprøvevist inspiceret, om kundefølgelser er dokumenteret i sagsstyringssystemet.</p>   | <p>Ingen bemærkninger.</p>  |

#### 4.4.4 Backup

Kontrolmål: At sikre beskyttelse mod tab af data.

|   | Etableret kontrol hos Curanet   | Udførte revisionshandlinger   | Konklusion  |
|---|---|---|---|
| 4.4.4.1<br><i>Backup – strategi</i>           | Der bliver udarbejdet backupstrategier ud fra den indgåede SLA med kunden. Der tages i udgangspunktet kun backup af kundeservere, såfremt dette er aftalt med kunden.                   | Deloitte har ved inspektion af den gældende SLA (6.3) påset, at udgangspunktet for backup heri er defineret.  | Ingen bemærkninger.   |
| 4.4.4.2<br><i>Backup – konfiguration</i>      | Curanet anvender en standardbackupkonfiguration til at tage backup af alle kundedata, medmindre andet er aftalt med kunden.   | Deloitte har ved forespørgsel hos nøglepersonale gennemgået standardkonfigurationen af backup.<br><br>Deloitte har for stikprøveudvalgte servere inspiceret, om backup bliver udført dagligt.                             | Vi har for en enkelt stikprøve konstateret, at der ikke er taget backup i første kvartal, 2019.<br><br>Ingen yderligere bemærkninger. |
| 4.4.4.3<br><i>Backup – ekstern opbevaring</i> | Backup spejles til underleverandører for at sikre, at der altid er produktionsdata tilgængelige i tilfælde af hændelser, der kunne kræve reetablering af systemer på en anden lokation. | Deloitte har ved forespørgsel hos nøglepersonale gennemgået opsætningen af backupreplikering til ekstern lokation<br><br>Deloitte har ved inspektion stikprøvevist påset, at replikering af backup bliver udført dagligt. | Ingen bemærkninger.   |
| 4.4.4.4<br><i>Backup – test</i>               | På baggrund af kundehenvendelse foretages test på en udvalgt server for at teste, at backupdata kan anvendes til reetablering.<br><br>Restore-testen godkendes af kunden.               | Deloitte har stikprøvevist inspiceret dokumentation for udført restore-test af backup i 2019 og påset, at denne er godkendt af kunden.  | Ingen bemærkninger.   |

#### 4.4.5 Drift og overvågning

Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

| Etableret kontrol hos Curanet                  |  | Udførte revisionshandlinger   | Konklusion   |
|--|--|---|--|
| 4.4.5.1<br><i>Driftsovervågning - generelt</i> | Der er etableret automatisk overvågning af servere og services, og ved afvigelser oprettes der automatisk en sag i overvågningssystemet. | Deloitte har ved forespørgsel hos nøglepersonale gennemgået opsætningen af driftsovervågning.<br><br>Deloitte har stikprøvevist påset, at afvigelser registreres i overvågningssystemet og behandles. | Ref. 4.4.4.2<br><br>Ingen yderligere bemærkninger. |

#### 4.4.6 Adgangskontrol og logisk sikkerhed

Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

|   | Etableret kontrol hos Curanet   | Udførte revisionshandlinger   | Konklusion  |
|---|---|---|---|
| 4.4.6.1<br><i>Brugerrettigheder - oprettelser</i>           | Interne brugere hos Curanet oprettes gennem faste oprettelsesprocedurer og på baggrund af forespørgsel fra leder.   | Deloitte har inspiceret adgangsstyringspolitikken og verificeret, at denne er ajourført i 2019.<br><br>Deloitte har stikprøvevist inspiceret, at oprettelse af brugere er sket på baggrund af en sag i sagsstyringssystemet, og at oprettelsen er bestilt eller godkendt af en leder. | Ingen bemærkninger.   |
| 4.4.6.2<br><i>Brugerrettigheder - nedlæggelser</i>          | Interne brugere nedlægges før eller på fratrådte medarbejders fratrædelsesdato, og det vurderes, om relevante password skal skiftes. Dette dokumenteres i sagsstyringssystemet. | Deloitte har stikprøvevist inspiceret, at fratrådte brugeres konti nedlægges i henhold til den oplyste procedure.   | Ingen bemærkninger.   |
| 4.4.6.3<br><i>Brugerrettigheder - udvidede rettigheder</i>  | Udvidede rettigheder er begrænset til ansatte hos Curanet med et arbejdsbetinget behov herfor.  | Deloitte har inspiceret listen over brugere, der er tildelt udvidede rettigheder på to interne Windows-domæner, og ved forespørgsel hos nøglepersonale verificeret, at kun brugere med et arbejdsbetinget behov er tildelt udvidet adgang   | Ingen bemærkninger.   |
| 4.4.6.4<br><i>Brugerrettigheder - periodisk revurdering</i> | Der foretages periodisk gennemgang af brugere med udvidede rettigheder, hvormed inaktive eller fratrådte brugere fjernes.   | Deloitte har stikprøvevist inspiceret dokumentation for, at periodisk gennemgang af brugere med udvidede adgange er gennemført i revisionsperioden.   | Vi kan konstatere, at den foreliggende dokumentation for udført revurdering ikke indeholder konklusionen på gennemgangen.<br><br>Vi har dog ved gennemgang af administrative brugere på de to Windows-domæner verificeret med CTO, at adgangene er godkendte og arbejdsbetingede.<br><br>Ingen yderligere bemærkninger. |

#### 4.4.6 Adgangskontrol og logisk sikkerhed

Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

| Etableret kontrol hos Curanet                  | Udførte revisionshandlinger  | Konklusion   |
|--|--|--|
| 4.4.6.5<br><i>It-sikkerhedslogning</i>         | Der er opsat logning af sikkerhedsmæssige hændelser på Curanets infrastruktur.   | Deloitte har stikprøvevist inspiceret dokumentation for, at der er opsat logning af sikkerhedsmæssige hændelser på infrastrukturen.<br><br>Vi har konstateret, at der sker logning af adgange i op til 30 dage. Vi har dog konstateret, at logs ikke er beskyttet mod manipulation eller sletning, ud over den underliggende backup.<br><br>Ingen yderligere bemærkninger.   |
| 4.4.6.6<br><i>Anvendelse af kodeord</i>        | Autentificering af brugere sker via de interne Windows-domæner, hvor kodeordskravene er defineret  | Deloitte har inspiceret konfigurationen af kodeord på de interne Windows-domæner og har bekræftet med den it-sikkerhedsansvarlige, at denne kodeordskonfiguration, herunder skift hver 180. dag, er godkendt af ledelsen.<br><br>Ingen bemærkninger.   |
| 4.4.6.7<br><i>Anvendelse af brugerprofiler</i> | Brugere er oprettet i de interne Windows-domæner, og alle anvender individuelle brugerprofiler på det interne netværk.<br>Der er sporbarhed på tilgang til kundeservere. | Deloitte har stikprøvevist inspiceret, at brugerprofiler, som benyttes af medarbejdere på relevante systemer og platforme, er personhenførbare.<br><br>Deloitte har stikprøvevist inspiceret log for tilgang til kundeservere og påset, at der er sporbarhed.<br><br>Ref. 4.4.6.5<br>Vi har konstateret, at medarbejdere har anvendt den indbyggede administrator, og at det arbejdsbetingede behov for anvendelsen ikke dokumenteres.<br><br>Ingen yderligere bemærkninger. |



#### 4.4.7 Anskaffelse og vedligeholdelse af systemsoftware

Kontrolmål: At sikre integriteten af driftssystemer.

|  | Etableret kontrol hos Curanet   | Udførte revisionshandlinger  | Konklusion  |
|--|---|--|---|
| 4.4.7.1<br><i>Konfigurationsbaseline – revurdering</i> | Der foretages en årlig revurdering af konfigurationsbaselinen.  | Vi har forespurgt til proceduren for årlig gennemgang af konfigurationsbaselines.  | Vi har konstateret for tilretning af konfigurationsbaselinen, at der ikke forefindes dokumenteret godkendelse og kvalitets sikring, herunder test inden implementering.<br><br>Ingen yderligere bemærkninger.   |
| 4.4.7.2<br><i>Konfigurationsbaseline – kontrol</i>     | Nye Windows-servere, der sættes i drift, er konfigureret i overensstemmelse med den aktuelle baseline, som er defineret i en række scripts. Denne baseline indeholder specifikke krav til kodeord og patching                                       | Deloitte har forespurgt til proceduren for opsætning af en ny Windows-server.<br><br>Deloitte har inspiceret opsætningen af én ny Windows-server med henblik på at konstatere, om kodeord og patching er opsat i overensstemmelse med den aktuelle baseline.   | Ingen bemærkninger.   |
| 4.4.7.3<br><i>Systemsoftware – patch management</i>    | Der foretages løbende opdatering af Windows- og Linux-servere. For Windows-platforme styres opdateringerne gennem WSUS, og for Linux-servere styres opdateringerne gennem Yum.<br><br>Patches til ESXi sker manuelt ud fra en vurdering af patches. | Deloitte har inspiceret Curanets patch management-procedurer for Windows, Linux og ESXi.<br><br>Deloitte har stikprøvevist inspiceret dokumentation for opdatering af Windows-og Linux-servere og påset, at der løbende installeres patches.<br><br>Deloitte har ved forespørgsel hos nøglepersonale gennemgået processen for patch af ESXi samt ledelsens valg af det nuværende patch-niveau. | Vi har konstateret, at flere stikprøveudvalgte servere ikke har været patchet med tilgængelige sikkerhedspatches igennem hele revisionsperioden.<br><br>Endvidere har vi konstateret, at politikken for patchning af Windows og Linux senest er opdateret i 2017. Vi er blevet oplyst om, at dette skyldes at patchprocessen er under opdatering.<br><br>Ingen yderligere bemærkninger. |

#### 4.4.8 Beredskabsplan

Kontrolmål: Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

|   | <b>Etableret kontrol hos Curanet</b>  | <b>Udførte revisionshandlinger</b>  | <b>Konklusion</b>   |
|---|---|---|---------------------|
| 4.4.8.1<br><i>Udarbejdet beredskabsplan</i> | Der er udarbejdet en overordnet beredskabsplan, som mindst én gang om året bliver opdateret og godkendt af Curanets ledelse.  | Deloitte har ved inspektion påset, at der er udarbejdet en beredskabsplan, som udgøres af en overordnet beredskabsplan og underliggende backuppolitik.<br><br>Deloitte har forespurgt, om beredskabsplanen er opdateret og godkendt i 2019. | Ingen bemærkninger. |
| 4.4.8.2<br><i>Test af beredskabsplan</i>    | Der udføres beredskabsøvelser mindst én gang årligt. I forbindelse med beredskabsøvelser foreligger dokumentation for handlinger foretaget i forbindelse med 'dry run' af beredskabsplan. | Deloitte har inspiceret playbook og mødenoter udarbejdet i forbindelse med en beredskabsøvelse, der er udført i perioden.   | Ingen bemærkninger. |

#### 4.4.9 Styring af leverandørydelser

Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

|  | <b>Etableret kontrol hos Curanet</b>   | <b>Udførte revisionshandlinger</b>  | <b>Konklusion</b>   |
|--|--|---|---------------------|
| 4.4.9.1<br><i>Styring af leverandørydelser</i> | Der foretages årlig opfølgning på underleverandører, hvor ledelsen foretager inspektion eller gennemgår revisionserklæringer, og eventuelle kontrolafvigelser bliver noteret,. | Deloitte har inspiceret dokumentation for Curanets gennemgang og opfølgning på deres underleverandørers revisionserklæringer.<br><br>Deloitte har forespurgt nøglepersonale om gennemført opfølgning på en ny underleverandør, og har fået oplyst, at Curanet har foretaget opfølgning i form af fysisk inspektion. | Ingen bemærkninger. |