www.pwc.dk

Cloud Factory

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2022 til 31. december 2022 i relation til Cloud Factorys it-drifts- og hosting-aktiviteter til kunder

Maj 2023

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Cloud Factorys it-drift og hosting-aktiviteter, 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 deres regnskaber.

Cloud Factory anvender GlobalConnect A/S til housing af primært og sekundært datacenter. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som GlobalConnect A/S varetager for Cloud Factory.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Cloud Factory bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af Cloud Factorys it-drift og hosting-aktiviteter, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2022 til 31. december 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til Cloud Factorys it-drift og hosting-aktiviteter var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret
   - De processer i både it-systemer og manuelle systemer, der er anvendt til styring af generelle it-kontroller
   - Relevante kontrolmål og kontroller udformet til at nå disse mål
   - Kontroller, som vi med henvisning til udformningen af Cloud Factorys it-drift og hosting-aktiviteter 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
   - Hvordan andre betydelige begivenheder og forhold end transaktioner behandles
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller

   (ii) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til Cloud Factorys it-drift og hosting-aktiviteter foretaget i perioden fra 1. januar 2022 til 31. december 2022

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til Cloud Factorys it-drift og hosting-aktiviteter, 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 generelle it-kontroller i relation til Cloud Factorys it-drift og hosting-aktiviteter, som den enkelte kunde måtte anse vigtigt efter sine 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 1. januar 2022 til 31. december 2022. Kriterierne anvendt for at give 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 udført 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 fra 1. januar 2022 til 31. december 2022.

Varde, den 31. maj 2023
CloudFactory

Svend Pedersen, CEO

2 Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2022 til 31. december 2022 i relation til Cloud Factorys it-drifts- og hosting-aktiviteter til kunder

Til: Cloud Factory, Cloud Factorys kunder og disses revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Cloud Factorys beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til Cloud Factorys it-drifts- og hosting-aktiviteter, der har behandlet kunders transaktioner i hele perioden fra 1. januar 2022 til 31. december 2022, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Cloud Factory anvender GlobalConnect A/S til housing af primært og sekundært datacenter. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som GlobalConnect A/S varetager for Cloud Factory.

Enkelte af de kontrolmål, der er anført i Cloud Factorys beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunder er hensigtsmæssigt udformet og fungerer effektivt sammen med Cloud Factorys kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Cloud Factorys ansvar

Cloud Factory er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, 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 opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Vores revisionsfirma anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Cloud Factorys beskrivelse samt om udformningen og funktionen af de 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, og de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at 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 sine it-drifts- og hosting-aktiviteter samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, 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 opnået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt egnetheden af de kriterier, som Cloud Factory har specificeret og beskrevet i ledelsens 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

Cloud Factorys 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 Cloud Factorys it-drifts- og hosting-aktiviteter, som hver enkelt kunde måtte anse for vigtige efter sine 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 ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af de generelle it-kontroller i relation til Cloud Factorys it-drifts- og hosting-aktiviteter, således som de var udformet og implementeret i hele perioden fra 1. januar 2022 til 31. december 2022, i alle væsentlige henseender er tilfredsstillende præsenteret, og

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 1. januar 2022 til 31. december 2022, 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 opnået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar 2022 til 31. december 2022.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne 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 Cloud Factorys it-drifts- og hosting-aktiviteter, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Aarhus, den 31. maj 2023
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Martin Roursgaard Nielsen
manager

3 Serviceleverandørs systembeskrivelse

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Cloud Factorys partnere og disses revisorer i overensstemmelse med kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos serviceleverandør, ISAE 3402. Beskrivelsen omfatter information om system- og kontrolmiljøet, som er etableret i og omkring Cloud Factorys drifts- og hostingydelser, der leveres til Cloud Factorys shared løsninger.

Nærværende beskrivelse indeholder beskrivelser af de anvendte procedurer til sikring af en betryggende afvikling af systemer. Formålet er at give tilstrækkelige informationer til, at partnernes revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet i forbindelse med revisors planlægning af revision i 2022.

3.2 Beskrivelse af Cloud Factorys ydelser

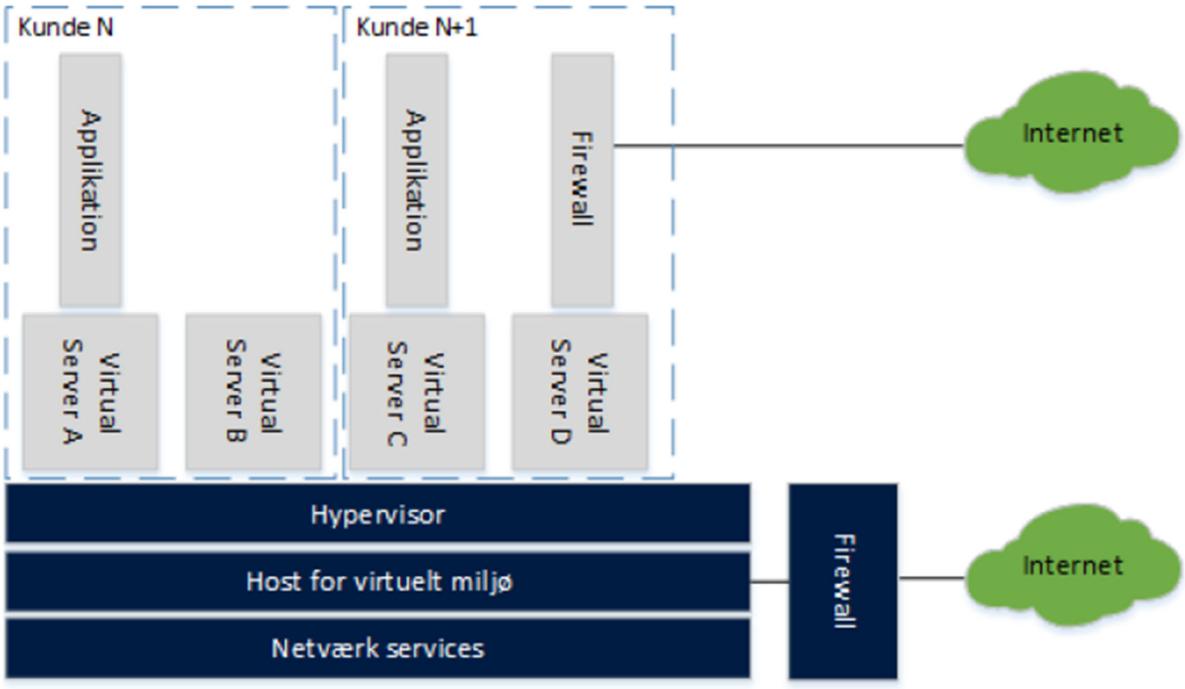
Cloud Factory er en dansk virksomhed, der tilbyder virtuel infrastruktur ud fra "cloud-filosofi", hvor mange forskellige brugere deles om de samme systemer, og dermed har mulighed for stor fleksibilitet på de leverede ydelser. Brugerne kan her bestille services, dvs. systemressourcer, softwarepakker etc. efter behov og i takt med, at deres forretning udvikles.

Cloud Factorys serviceydelser er cloud-løsninger, som primært er baseret på Nutanix Hyperconverged Infrastructure. Kundekredsen er it-servicevirksomheder, også benævnt som partnere, som leverer deres ydelser til de endelige slutkunder på Cloud Factorys teknologiske platform. Nærværende erklæring omfatter således følgende serviceydelser leveret af Cloud Factory:

- Infrastructure-as-a-service (IaaS)
    - Infrastruktur i form af netværk og en platform for oprettelser af virtuelle servere

Cloud Factorys serviceydelser kan ikke sammenlignes med en traditionel struktur for hosting, idet Cloud Factory alene leverer den tekniske platform, hvorfra partnerne kan bygge deres hostingvirksomhed. Dette

kan overordnet set illustreres således:



De blå områder er Cloud Factorys leverance og ansvar, mens de grå områder er partnernes leverance og ansvar.

Nærværende erklæring omfatter ikke it-hosting-virksomhedernes/partnernes leverancer og ansvar.

3.3 Ansvar og organisering hos Cloud Factory

Cloud Factory har i 2022 været ejet af Jacob V. Schmidt ApS, Mark R. Ibsen ApS og CF SPV ApS og beskæftiger ca. 40 medarbejdere. Produktansvaret er placeret som følger:

- CEO (Chief Executive Officer)
- CCO (Chief Commercial Officer), ansvarlig for salg, marketing, indkøb mv.
- CFO (Chief Operations Officer), ansvarlig for økonomi, partnerkontrakter, SLA, risikostyring mv.
- CTO (Chief Technical Officer), ansvarlig for teknik, nyudvikling, overvågning, drift, support mv.

Cloud Factory anvender enkelte underleverandører til udførelse af meget specifikke opgaver. Følgende områder er Cloud Factorys ansvar, men de daglige arbejdsopgaver/sikringsforanstaltninger varetages af følgende underleverandører:

- Housing af primært og sekundært datacenter er outsourcet til dels GlobalConnect A/S og dels Bulk Data Centers Dk01 ApS

3.4 Risikostyring hos Cloud Factory

Cloud Factory har fastsat processer for risikovurdering af sin forretning. Formålet med it-risikovurderingen er at sikre, at de risici, som er forbundet med de services, som Cloud Factory stiller til rådighed, er minimeret til et acceptabelt niveau. It-risikovurderingen revurderes med fastsatte intervaller og minimum i forbindelse med, at der indføres nye services.

It-risikovurderingen gennemføres af de ansvarlige for de enkelte afdelinger samt øvrige relevante medarbejdere og godkendes af Cloud Factorys direktør.

3.5 Kontrolframework, kontrolstruktur og kriterier for kontrolimplementering

Cloud Factorys it-sikkerhedspolitik er gældende for alle medarbejdere og er etableret med henblik på at skabe et styringsværktøj for hensigtsmæssig og betryggende drift af Cloud Factorys kerneydelser, som tilbydes over for partnerne. Der sker løbende forbedring af såvel fysisk som logisk sikkerhed, driftsafvikling, beredskabsplanlægning og support af it-infrastrukturen, samt udførelse og dokumentation af de etablerede kontroller.

Cloud Factory anvender et kontrolframework baseret på ISO 27001:2017 samt best practice for minimering af risici i forbindelse med hosting-ydelser på shared infrastruktur. Med udgangspunkt i denne kontrolmodel er system- og kontrolmiljøet for ydelserne etableret på nedenstående udvalgte kontrolområder af ISO 27001:2017:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Personalesikkerhed
- Mediehåndtering
- Adgangsstyring
- Fysisk sikring og miljøsikring
- Driftssikkerhed
- Kommunikationssikkerhed
- Styring af leverandørydelser.

Cloud Factory har etableret ledelsesmæssige kontroller, som sikrer, at de etablerede procedurer efterleves dels hos medarbejderne og dels hos relevante underleverandører. Dette er etableret ved, at relevante underleverandører skal bekræfte, at de efterlever samarbejdsaftalen og dermed Cloud Factorys it-sikkerhedspolitik.

3.6 Etableret kontrolmiljø

Cloud Factory har en overordnet målsætning om at levere stabil og sikker it-drift til sine partnere. Målsætningen er udmøntet i definerede politikker på disse fire områder:

- Risikopolitik: Der er fastlagt processer for løbende risikovurdering af virksomhedens forretning. Formålet er at sikre, at de risici, som er forbundet med de services og ydelser, som virksomheden stiller til rådighed, er reduceret til et acceptabelt niveau.

- It-sikkerhedspolitik: Politikken omfatter alle medarbejdere og alle leverancer. Der foretages regelmæssigt opdatering af både politikker, procedurer og den operationelle drift.

- Kontrolprocedurer: Der er indført politikker og procedurer for overvågning og support for at sikre, at virksomhedens leverancer er ensartede og gennemskuelige.

- Informationsstyring: Cloud Factory beskytter den information og viden, der løbende bygges op gennem daglig sagsbehandling, vedligeholdelse af databaser og udvikling af nye produkter og tiltag.

Nedenfor er de enkelte kontrolområder, etablerede procedurer og kontroller nærmere beskrevet.

3.6.1 Informationssikkerhedspolitikker

Formål

Ledelsen har defineret politikker og retningslinjer på baggrund af en vurdering af it-risici i Cloud Factorys forretning, herunder at politikker og vejledning er kommunikeret til hele Cloud Factory og virksomhedens underleverandører.

Anvendte procedurer og kontroller inden for informationssikkerhed

Cloud Factory har defineret en lang række skriftlige procedurer til understøttelse af selskabets mål om at levere stabil og sikker it-drift til dets partnere. Medarbejdere samt relevante underleverandører er bekendt med disse procedurer, og ledelsen følger op på, at procedurerne efterleves, og at de afspejler dagligdagen hos Cloud Factory. Nedenfor er nævnt de væsentligste dokumenter.

Risikovurdering

Cloud Factory har gennemført en risikovurdering. Virksomheden har i den forbindelse vurderet driftskritiske aktiver og informationsaktiver, hvor brud på tilgængelighed, fortrolighed eller integritet hver for sig og individuelt betragtet ikke er acceptabelt for organisationens forretningsmæssige virke.

Cloud Factorys analyser er dog reduceret til alene at omfatte følgende elementer:

- Konsekvensvurdering
- Sandsynlighed
- Risiko.

Risikovurdering opdateres ved ændringer i virksomhedens forhold, fx ved ændrede leverancer af service. Vurdering skal ske minimum én gang årligt.

It-sikkerhed

Baseret på resultaterne af risikovurderingen har Cloud Factory udarbejdet relevante politikker og retningslinjer, som er tilgængelige for alle medarbejdere hos Cloud Factory. Disse bliver løbende opdateret efter behov. Følgende hovedområder er behandlet i dokumentet it-sikkerhed:

- Fysisk sikkerhed: Omfattende adgang til kontorer, underleverandører og databærende udstyr
- Logisk sikkerhed: Omfattende administration af adgang og rettigheder samt krav til sikkerhedsparametre
- Personale og underleverandører: Retningslinjer for håndtering af it-sikkerhed over for personale og relevante underleverandører ved ansættelse og fratrædelse
- Beredskab: Retningslinjer for håndtering af brud på it-sikkerhed, problem management og beredskab ved angreb på onlinesystemer.

3.6.2Organisering af informationssikkerhed

Formål

Ledelsen har placeret ansvar for drift og it-sikkerhed og sikret, at relevante informationer stilles til rådighed for medarbejdere og underleverandører.

Anvendte procedurer og kontroller inden for intern organisering

Alle ansvarsområder for informationssikkerhed er defineret og fordelt. Der er en fast procedure for oprettelse og vedligehold af brugerroller for at undgå uautoriseret og utilsigtet anvendelse, ændring og misbrug af aktiver. Der er kontakt med relevante myndigheder og organisationer som fx DKCERT ved behov.

Relevante Cloud Factory-leverandører og samarbejdspartnere er kontraktmæssigt forpligtet til at overholde firmaets it-sikkerhedspolitik og til at sætte sig ind i ændringerne, hvis Cloud Factory opdaterer politikken.

3.6.3Personalesikkerhed

Formål

Ledelsen har fastsat retningslinjer for rekruttering, fastholdelse og fratrædelse af personale, herunder retningslinjer, der skal sikre, at kompetencer vedligeholdes, og selskabets it-sikkerhed efterleves.

Anvendte procedurer og kontroller inden for personalesikkerhed

Cloud Factory har fastsatte retningslinjer for håndtering af personale. Følgende retningslinjer skal særligt fremhæves:

Før ansættelsen

Medarbejdernes og samarbejdspartnernes kontrakter beskriver de pågældendes og organisationens ansvar for informationssikkerheden, og at denne er afstemt med Cloud Factorys retningslinjer.

Eventuel efterprøvning af jobkandidaters baggrund skal udføres i overensstemmelse med relevante love, forskrifter og etiske regler. Dette gælder både for Cloud Factory og for virksomhedens samarbejdspartnere.

Under ansættelsen

Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med Cloud Factorys politikker og procedurer. Alle organisationens medarbejdere og relevante samarbejdspartnere bliver løbende informeret og gjort bevidste om Cloud Factorys informationssikkerhed ved hjælp af uddannelse og øvelser.

Efter ansættelsen

Informationssikkerhedsansvar og -forpligtelser, som også gælder efter ansættelsens ophør eller ændring, er defineret og kommunikeret til medarbejderen/leverandøren og håndhæves af virksomheden.

3.6.4Mediehåndtering

Formål

Ledelsen har fastsat retningslinjer for håndtering af databærende medier.

Anvendte procedurer og kontroller inden for databærende medier

Virksomheden håndterer ikke følsomme data på håndbårne medier som fx USB-drev og DVD.

Ved fysisk transport af medier med følsomme data skal anvendes fragtmand. Medierne skal beskyttes mod uautoriseret adgang, misbrug og ødelæggelse under transporten.

Ved udskiftning af forældede eller beskadigede harddiske vil den udskiftede harddisk enten blive sendt tilbage til leverandøren af NetApp eller HPE-udstyret for data clearing, alternativt udfører Cloud Factory selv udskiftningen, og placerer harddisken i en lukket container, som håndteres af firmaet Marius Pedersen, som via vores kontrakt håndterer harddisk makulering på professionel vis.

3.6.5Adgangsstyring

Formål

Ledelsen har fastsat retningslinjer for administration af adgang til Cloud Factorys systemmiljøer, herunder tildeling af rettigheder, således at en passende adskillelse af uforenelige funktioner er etableret.

Anvendte procedurer og kontroller inden for adgangsstyring

Cloud Factory har fastsat retningslinjer for tildeling af adgang og rettigheder til de anvendte systemmiljøer. Det skal i den forbindelse nævnes, at Cloud Factory ikke har adgang til data og informationer på de af partnerne oprettede virtuelle servere.

Adgang til systemmiljøerne sker gennem standard-Microsoft autentifikationsteknikker ved angivelse af unikke bruger-id'er og tilhørende password. Krav til passwords følger best practice i Danmark.

Adgangen tildeles dels gennem faste linjer og dels ved brug af internettet. Adgang fra internet til interne netværk foregår gennem firewalls.

Al kundeadgang, dvs. ekstern brugeradgang, til individuelle hostede miljøer foregår gennem VPN, Virtual Private Network, som en punkt-til-punkt-forbindelse via internettet eller via MLPS, Multiprotocol Label Switching-forbindelse eller via Console adgang i Partner Portalen.

Personlige arbejdsstationer hos Cloud Factory er sat op til at anvende screensavere med påkrævet anvendelse af adgangskode.

Alle personer med adgang til Cloud Factorys miljøer skal underskrive en fortrolighedserklæring, som forpligter til fortrolighed om alle informationer, som den person måtte få kendskab til. Erklæringen gælder både under og efter ansættelsesforholdet. Kravet om fortrolighed gælder:

- Alle medarbejdere
- Alle medarbejdere ved underleverandører (med adgang til virksomhedens it-systemer).

Det påhviler Cloud Factorys ledelse at overvåge tildelte adgange og rettigheder regelmæssigt samt at sikre, at medarbejderne overholder fortrolighedserklæringen og griber ind, hvis der sker overtrædelser.

3.6.6Fysisk sikring og miljøsikring

Formål

Ledelsen har fastsat retningslinjer for administration af adgang til Cloud Factorys fysiske faciliteter, herunder udstyr, som placeres hos underleverandører.

Anvendte procedurer og kontroller inden for fysiske sikringsforanstaltninger

Cloud Factory har defineret retningslinjer for betryggende fysiske sikringsforanstaltninger.

Adgang til kontorer

Fysisk adgang til Cloud Factory sker uden for normal åbningstid med udleveret nøgle og adgangsbrik. Gæster ledsages altid af en medarbejder.

Housing ved underleverandører

Cloud Factorys servere er fysisk placeret ved GlobalConnect og BULK for henholdsvis primært og sekundært datacenter.

Det er underleverandørernes opgave at sikre et betryggende fysisk miljø for Cloud Factorys hosting-system og virksomhedens partneres og slutkunders data. Servere, services, data og andre informationer er beskyttet mod skade fra brand, vand, temperatur, strømsvigt, hærværk, tyveri mv.

Ved underleverandøren findes der nødstrømsanlæg og dieselgenerator. Der er redundant køling og brandslukningsanlæg. Alt udstyr med Cloud Factorys kundedata er placeret i rackskabe inden for aflåste hegn.

Adgang til serverrummene er begrænset med adgangskort med tilhørende kode samt enkelte fysiske nøgler. Kun autoriserede personer har adgang til serverrummene.

Housing af produktion

Servere er fysisk placeret ved housing-leverandøren GlobalConnect A/S.

Adgangskort til lejemålet ved GlobalConnect kan kun udstedes ved bestilling fra direktionen. Cloud Factory følger regelmæssigt op på, hvilke personer der har adgang til udstyr hos GlobalConnect A/S.

Adgang for teknikere ansat ved underleverandører følger GlobalConnects faste procedurer, og adgang gives kun efter aftale med Cloud Factory i hvert enkelt tilfælde.

Gæster har kun adgang, hvis de ledsages af en medarbejder.

Cloud Factory modtager årligt en 3402-erklæring fra GlobalConnect A/S på deres sikringsforanstaltninger.

Det skal fremhæves, at de fysiske sikringsforanstaltninger hos GlobalConnect A/S ikke er en del af denne erklæring.

Housing af Disaster Recovery
Cloud Factorys Disaster Recovery er fysisk placeret på to forskellige lokationer ved to forskellige housing leverandører. Til formålet anvendes GlobalConnect A/S samt BULK datacenter DK01.

Adgangskort til lejemålet ved GlobalConnect og BULK kan kun udstedes ved godkendelse og bestilling via navngivne ledende medarbejdere. Cloud Factory følger regelmæssigt op på, hvilke personer der har adgang til udstyr hos GlobalConnect A/S og BULK datacenter DK01.

Adgang for teknikere ansat ved underleverandører følger GlobalConnects og BULKs faste procedurer, og adgang gives kun efter aftale med Cloud Factory i hvert enkelt tilfælde.

Gæster har kun adgang, hvis de ledsages af en medarbejder.

Cloud Factory modtager årligt en 3402-erklæring fra GlobalConnect A/S på deres sikringsforanstaltninger samt en ISO 27001 fra BULK datacenter DK01 på deres sikringsforanstaltninger.

3.6.7Driftssikkerhed

Formål
Ledelsen har fastsat retningslinjer for sikring af en betryggende driftssikkerhed i overensstemmelse med selskabets it-sikkerhedspolitik og indgåede aftaler med partnere.

Anvendte procedurer og kontroller inden for driftssikkerhed
Cloud Factory har defineret driftsprocedurer, som er gjort tilgængelige for alle brugere, der har behov. Systemdokumentationen og beskrivelsen af de interne rutiner opdateres ved væsentlige ændringer i driftsprocesser og systemer.

Styring og overvågning af driften sker i flere forskellige værktøjer til overvågning af driften, herunder overvågning af, at kunderne får den leverance, der er indgået aftale om. Følgende værktøjer anvendes:

- PRTG – værktøj til overvågning af systemmiljøer
- Jira Service Desk – ekstern incident-håndtering
- Jira – Projekt- og opgavestyring samt intern incident-håndtering
- Dropbox – dokumentstyring.

Alarmer fra disse værktøjer tilgår teknisk afdelings driftsgruppe alt efter hændelse, således at der altid vil være en driftsmedarbejder, som kan tage hånd om eventuelle fejl og alarmer.

Logning og overvågning
Der foregår automatiseret overvågning døgnet rundt. Processen følges af Cloud Factory driftspersonale, som modtager alarmerne og behandler dem løbende.

Systemadministrators handlinger bliver logget dels på host-serverne og dels i de administrationsværktøjer, som Cloud Factory stiller til rådighed. Loggen gennemgås regelmæssigt af den ansvarlige for drift og support. Den er beskyttet mod manipulation og uautoriseret adgang. Alle gennemførte konfigurationsændringer og opdateringer i udstyret skal være registreret.

Håndtering af incidents
Cloud Factory har værktøjer og procedurer for håndtering af incidents og hændelser, dels identificeret af partnerne og dels af internt driftspersonale. Disse håndteres ud fra fastsatte SLA'er, og der gennemføres en regelmæssig ledelseskontrol af, at de fastsatte retningslinjer efterleves af support- og driftspersonalet.

Styring af driftssoftware

Der er implementeret procedurer til styring af opdatering og vedligeholdelse af de virtuelle miljøer.

Ændringskontrol – patch management

Cloud Factory har udformet en procedurer for at håndtere patches. Denne procedure håndteres af virksomhedens third-level-support og er dokumenteret i et internt overvågnings- og supportdokument.

Ændringskontrol – change management

Cloud Factory har udformet en procedure for at håndtere changes. I forbindelse med changes er der nedsat et Change Advisory Board, som skal være med til at prioritere opgaverne. Changes bliver analyseret og testet af third-level-support, inden Change Advisory Board skal acceptere eller forkaste den foreslåede løsning. Når changen accepteres, tages der stilling til, hvad der kræves, for at den kan implementeres. Alt dette er dokumenteret i et internt dokument for overvågning og support.

Sårbarhedsstyring

Cloud Factory modtager løbende informationer om tekniske sårbarheder, evaluerer dem og iværksætter passende foranstaltninger for at håndtere den tilhørende risiko.

Disaster recovery

Cloud Factory tager snapshots af virtuelle systemmiljøer hver anden time og gemmer dem i 24 timer på SSD for lynhurtig recovery. Derudover tages der snapshots af virtuelle systemmiljøer én gang i døgnet, som gemmes på to forskellige lokationer. Disaster recovery-proceduren er tilrettelagt, således at restore kan udføres på internt serverniveau. Der foretages regelmæssig test af, at restore kan gennemføres. Cloud Factory er ikke ansvarlig for in-guest-backup af etablerede servere, databaser og applikationer, som de enkelte partnere måtte have installeret på den delte infrastruktur.

3.6.8 Kommunikationssikkerhed

Formål

Ledelsen har fastsat retningslinjer for administration af netværk og kommunikation.

Anvendte procedurer og kontroller inden for kommunikationssikkerhed

Cloud Factory har udformet procedurer for at håndtere patches, changes og incidents. Disse procedurer håndteres af virksomhedens third-level-support og er dokumenteret i et internt overvågnings- og supportdokument som nævnt ovenfor.

Cloud Factory har installeret en firewall for at beskytte indholdet på egne virtuelle servere og infrastrukturen generelt.

Cloud Factorys systemer er sat op, så ingen slutkunder deler netværk. Kun udvalgte brugere i third-level-support ved Cloud Factory kan logge på det kritiske netværksudstyr.

Ændringskontrol – patch management

Cloud Factory har udformet procedurer for at håndtere patches. Denne procedure håndteres af virksomhedens third-level-support og er dokumenteret i et internt overvågnings- og supportdokument.

Ændringskontrol – change management

Cloud Factory har udformet procedurer for at håndtere changes. I forbindelse med changes er der nedsat et Change Advisory Board, som skal være med til at prioritere opgaverne. Changes bliver analyseret og testet af third-level-support, inden Change Advisory Board skal acceptere eller forkaste den foreslåede løsning. Når changen accepteres, tages der stilling til, hvad der kræves, for at den kan implementeres. Alt dette er dokumenteret i et internt dokument for overvågning og support.

3.6.9Styring af leverandørydelser

Formål

Ledelsen har fastsat retningslinjer for styring af underleverandører, herunder at disse efterlever de fastsatte retningslinjer hos Cloud Factory.

Anvendte procedurer og kontroller inden for leverandører

For hver enkelt leverandør, som kan få adgang til at behandle, lagre, kommunikere eller levere ydelser til Cloud Factory, aftaler virksomheden relevante krav til leverandørens overholdelse af informationssikkerheden.

Cloud Factory overvåger og gennemgår regelmæssigt de modtagne leverandørydelser. Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, procedurer og kontroller, skal styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer er, og til en revurdering af risici.

3.7 Supplerende information om det etablerede kontrolmiljø og komplementerende kontroller

3.7.1 Forhold, som skal iagttages af partnernes revisorer

Levering af serviceydelser

Ovenstående systembeskrivelse af kontroller er baseret på Cloud Factorys standardaftalebetingelser for IaaS-ydelser. Partnernes egne revisorer bør vurdere, om denne erklæring kan anvendes, og selv afdække eventuelle andre risici, der vurderes som væsentlige for aflæggelse af partnernes årsregnskaber. Samme forhold gør sig gældende for en partners kunde – "slutkunden".

Partnerne skal således selv etablere sikringsforanstaltninger og kontroller på de virtuelle miljøer, servere, databaser og applikationer, som bygges på Cloud Factorys platform. Områder, som skal kontrolleres, er følgende:

- Brugeradministration til servere, databaser og applikationer
- Fortrolighed på og omkring slutkunders data
- Backup af servere, databaser og applikationer
- Driftsovervågning af servere, databaser og applikationer
- Patch management- og change management-servere, -databaser og -applikationer
- Beredskabsstyring af servere, databaser og applikationer.

De fysiske sikringsforanstaltninger hos GlobalConnect A/S og BULK datacenter DK01

Partnernes revisorer skal selv vurdere risici i relation til de fysiske sikringsforanstaltninger hos underleverandørerne og om nødvendigt indhente deres ISAE 3402- eller tilsvarende erklæring på deres housing-miljøer.

Efterlevelse af relevant lovgivning

Cloud Factory har tilrettelagt procedurer og kontroller således, at de områder, som er Cloud Factorys ansvar, efterleves betryggende. Cloud Factory er ikke ansvarlig for servere, databaser og applikationer, som afvikles på den delte infrastruktur, og som følge af dette omfatter denne erklæring ikke sikkerhed for, at der er etableret betryggende kontroller i disse systemer, herunder at partnerne og deres kunder efterlever bogføringsloven, persondataloven eller anden relevant lovgivning.

4. Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", og de yderligere krav, der er gældende i Danmark.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos kunder er ikke omfattet af vores testhandlinger.

Vores test af funktionaliteten har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået.

4.2 Testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrollers funktionalitet er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af, og stillingtagen til, rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontrollerne er implementeret og har fungeret i perioden fra 1. januar 2022 til 31. december 2022. Dette omfatter bl.a. vurdering af patching-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af udstyr og lokaliteter.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

A.5 kontrolmål: Informationssikkerhedspolitik

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
5.1.1	**Politikker for informationssikkerhed** Cloud Factory har udarbejdet en skriftlig it-sikkerhedspolitik, som vedligeholdes og godkendes af ledelsen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået informationssikkerhedspolitikkens tilstrækkelighed. Vi har påset, at ledelsen har godkendt it-sikkerheds-politikken.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
5.1.2	**Gennemgang af politikker for informationssikkerhed** Cloud Factory har udarbejdet en skriftlig it-sikkerhedspolitik, som vedligeholdes på årlig basis.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at it-sikkerhedspolitikken som minimum er revurderet én gang årligt. Endvidere har vi påset, at den forefindes let tilgængelig for medarbejderne.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.6 kontrolmål: Organisering af informationssikkerhed

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
6.1.1	**Roller og ansvarsområder for informationssikkerhed** Cloud Factory har defineret roller og ansvar for væsentlige forhold i deres it-sikkerhedsdokument. Der er – ud fra organisationens størrelse – defineret roller til de enkelte medarbejdere. Cloud Factory er dog karakteriseret ved i høj grad at anvende underleverandører til den praktiske udførelse af opgaverne.	Vi har overordnet drøftet ansvarsfordelingen med ledelsen. Vi har påset, at det organisatoriske ansvar for væsentlige forhold er dokumenteret i it-sikkerheds-politikken.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
6.1.2	**Funktionsadskillelse** Der er etableret adskillelse af funktioner, fx ved at ikke alle er administratorer og ved begrænsning af adgang til centrale dokumenter i selskabets dokumentstyringsværktøj.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået adgange til selskabets dokumentstyringsværktøj og brugere med administrative rettigheder, til verificering af at adgange er begrundet i et arbejdsbetinget behov.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.7 Kontrolmål: Personalesikkerhed

Formål: At sikre, at medarbejdere forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.1.1	**Screening** Cloud Factory har i deres rekrutteringspolitik defineret krav til efterprøvelse af jobkandidaternes kvalifikationer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, i forbindelse med efterprøvelse af jobkandidaternes kvalifikationer. Vi har gennemgået rekrutteringspolitikken for definerede krav til efterprøvelse af kvalifikationer. Vi har ved inspektion kontrolleret, at der foretages screening af jobkandidaternes kvalifikationer.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
7.1.2	**Ansættelsesvilkår og betingelser** Cloud Factory har i deres rekrutteringspolitik defineret krav til henholdsvis medarbejdere og underleverandører.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået rekrutteringspolitikken samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
7.2.1	**Ledelsesansvar** Cloud Factory har i it-sikkerhedspolitikken anført retningslinjer for medarbejdernes og samarbejdspartnernes introduktion til Cloud Factorys retningslinjer for informationssikkerhed.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået it-sikkerhedspolitikken samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
7.2.2	**Bevidsthed om uddannelse og træning i information sikkerhed** Cloud Factory har i it-sikkerhedspolitikken anført retningslinjer for medarbejdernes og samarbejdspartnernes bevidsthed om Cloud Factorys informationssikkerhed.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har overordnet drøftet styring af informationssikkerheden med ledelsen. Vi har gennemgået seneste tiltag inden for uddannelse samt træning vedrørende informationssikkerhed.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.7 Kontrolmål: Personalesikkerhed

Formål: At sikre, at medarbejdere forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
7.2.3	**Sanktioner** Der skal være en formel og kommunikeret disciplinær proces på plads for at gribe ind over for medarbejdere, der har begået et brud på informationssikkerheden.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at en disciplinær proces er på plads og er blevet kommunikeret til medarbejderne for at sikre, at alle medarbejdere er opmærksomme på konsekvenserne af at begå et brud på sikkerhedspolitikken.	Vi har ved vores test konstateret at der ikke forefindes en formaliseret procedure for sanktioner for brud på informationssikkerhed. Vi er blevet informeret om at dette er tilføjet efterfølgende. Vi har ikke konstateret yderligere væsentlige afvigelser.
7.3.1	**Ansættelsesforholdets ophør og ændring** Ved fratrædelse vil medarbejdernes forpligtelser angående tavshedspligt og fortrolighed være omfattet af kontrakten.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med ansættelsesophør og -ændringer. Vi har inspiceret, at medarbejderne via deres kontrakter er omfattet af tavshedspligt og fortrolighed.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.8 kontrolmål: Styring af aktiver

Formål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
8.1.1	**Fortegnelse over aktiver** Aktiver forbundet med informations- og informationsbehandlingsfaciliteter skal identificeres, og en fortegnelse over disse aktiver skal udarbejdes og vedligeholdes.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at tilstrækkelige kontroller er på plads for at sikre dokumentation og vedligeholdelse af beholdningen af aktiver.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
8.3.1	**Styring af bærbare medier** Cloud Factory har fastsat retningslinjer for håndtering af databærende medier.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for styring af bærbare medier. Vi har inspiceret retningslinjerne for håndtering af databærende medier.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.9 kontrolmål: Adgangsstyring

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
9.1.1	**Politik for adgangsstyring** En adgangskontrolpolitik skal etableres, dokumenteres og revideres baseret på forretnings- og informationssikkerhedskrav.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har kontrolleret, at retningslinjer for adgangskontrol er etableret, gennemgået og godkendt.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
9.1.2	**Adgang til netværk og netværkstjenester** Brugere skal kun have adgang til det netværk og de netværkstjenester, som de specifikt har fået tilladelse til at bruge.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Ved kontrol af stikprøver har vi verificeret, at der gives adgang til netværks- og netværkstjenester baseret på medarbejdernes jobfunktion og ledergodkendelser.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
9.2.1	**Brugerregistrering og -afmelding** Cloud Factory har defineret procedurer for oprettelse og nedlæggelse af brugere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der anvendes i forbindelse med brugeroprettelser og nedlæggelser. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved inspektion gennemgået brugeroprettelserne og nedlæggelser foretaget i perioden.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
9.2.3	**Styring af privilegerede adgangsrettigheder** Cloud Factory har i interne procedurer defineret retningslinjer for tildeling af privilegeret adgang og rettigheder til medarbejdere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.9 kontrolmål: Adgangsstyring

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

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
9.2.5	**Gennemgang af brugerrettigheder** Cloud Factory har defineret en procedure for periodisk gennemgang af brugere på kvartalsvis basis.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med den periodiske gennemgang af brugere. Vi har gennemgået procedurerne for brugeradministration, herunder it-sikkerhedspolitikken, samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har foretaget stikprøvevis kontrol af, at kvartalsvise gennemgange foretages.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
9.4.2	**Procedurer for sikker log-on** Adgang til systemer og funktioner kontrolleres af autorisationsfunktioner i Microsoft-systemer. Adgang håndteres gennem log-on til Windows domains, og tildeling af rettigheder sker gennem tilknytning af sikkerhedsgrupper i Active Directory.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for procedurer for sikker log-on. Vi har inspiceret opsætningen af Windows Active Directory.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
9.4.3	**System til administration af adgangskoder** Cloud Factory har defineret en politik for anvendelse af passwords.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for system til administration af adgangskoder. Vi har inspiceret politikken for anvendelse af passwords.	Vi har ved vores test konstateret, at systemindstillinger for krav til password ikke er i overensstemmelse med anbefalinger om minimumskrav fra Digitaliseringsstyrelsen. Vi har ikke konstateret yderligere væsentlige afvigelser.

A.11 kontrolmål: Fysisk sikring og miljøsikring

Formål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
11.1.1	**Fysisk perimetersikring** Sikkerhedsperimetre skal defineres og bruges til at beskytte områder, der indeholder enten følsomme eller kritiske informations- og informationsbehandlingsfaciliteter. Alle primære systemer hos Cloud Factory er placeret hos GlobalConnect, der varetager housing af servere og systemer. Adgang til udstyr tildeles kun på baggrund af godkendelse heraf.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for fysisk adgangskontrol.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
11.1.2	**Fysisk adgangskontrol** Sikre områder skal beskyttes af passende adgangskontrol for at sikre, at kun autoriseret personale har adgang. Alle primære systemer hos Cloud Factory er placeret hos GlobalConnect, der varetager housing af servere og systemer. Adgang til udstyr tildeles kun på baggrund af godkendelse heraf.	Vi inspicerede, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at adgange til Cloud Factorys udstyr hos underleverandøren er begrænset til godkendt personale.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
11.1.3	**Sikring af kontorer, lokaler og faciliteter** Fysisk sikring af kontorer, lokaler og faciliteter skal designes og anvendes.	Vi inspicerede, at en formel fysisk adgangs- og sikkerhedspolitik vedligeholdes, gennemgås og godkendes. Vi har inspiceret, at Cloud Factory har implementeret passende adgangskontroller for at beskytte fysiske faciliteter.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.11 kontrolmål: Fysisk sikring og miljøsikring

Formål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
11.2.1	**Placering og beskyttelse af udstyr** Udstyr skal placeres og beskyttes for at reducere risici fra miljøtrusler og -farer og muligheder for uautoriseret adgang	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har kontrolleret, at Cloud Factory har fastlagt retningslinjer for beskyttelse mod brand, vand og varme. Vi har endvidere kontrolleret, at Cloud Factory har indhentet revisionsrapport fra underleverandør med henblik på at sikre, at tilsvarende krav er opfyldt på områder, der er omfattet af outsourcing.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.12 Kontrolmål: Driftsikkerhed

Formål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter og beskytte mod tab af data

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
12.1.1	**Dokumenterede driftsprocedurer** Cloud Factory har etableret skriftlige driftsprocedurer for deres kerneforretning.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
12.1.2	***Ændringsstyring*** Cloud Factory har defineret en procedure for change management, som anvendes ved alle ændringer, der kræver test og/eller service-vinduer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået change management-procedurernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur. Vi har ved stikprøvevis inspektion af ændringer gennemgået følgende: • Registrering af ændringsanmodninger i det dertil etablerede system • Dokumenteret test af ændringer, herunder godkendelse. • Funktionsadskillelse • Godkendelse opnået før implementering Dokumenteret plan for tilbagerulning, hvor relevant.	Vi har konstateret at ikke alle ændringer er ledelsesgodkendt før implementering. Vi ikke konstateret yderligere væsentlige afvigelser.
12.3.1	**Backup af information** Sikkerhedskopier af information, software og systembilleder skal tages og testes løbende i overensstemmelse med en aftalt backuppolitik.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har efterset, at der er fastsat krav til backup i kontrakten med underleverandører, der leverer ydelser, hvor backup er relevant. Vi har inspiceret, at der er udført en fuld gendannelsestest af it-miljøer.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.12 Kontrolmål: Driftsikkerhed

Formål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter og beskytte mod tab af data

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
12.4.1	**Hændelseslogning** Cloud Factory har defineret en procedure for overvågning af driften. Overvågning indeholder interne hændelser fra driftsafdelingen. Derudover omfatter overvågningen alarmer fra de anvendte systemmiljøer. Der sker en kontinuerlig overvågning af systemmiljøerne, ligesom der fra ledelsen følges op på efterlevelse af Cloud Factorys retningslinjer. Der er p.t. ikke implementeret logning på trafik gennem firewalls.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for hændelseslogning. Vi har inspiceret proceduren for overvågning af driften samt dokumentation for overvågning af hændelser.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
12.4.2	**Beskyttelse af logoplysninger** Logfiler, som p.t. forefindes hos Cloud Factory, er passwordbeskyttede.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for beskyttelse af logoplysninger. Vi har inspiceret, at logfiler er passwordbeskyttede.	Vi har konstateret at logning ikke er tilstrækkeligt beskyttet i forhold til integritet og tilgængelighed. Vi har ikke konstateret yderligere væsentlige afvigelser.
12.4.3	**Administrator og operatørlog** Der er opsat logning på administratorhandlinger, og operatørloggen gennemgås regelmæssigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for administrator og operatørlog. Vi har inspiceret, at der er opsat logning på administratorhandlinger, og at operatørloggen gennemgås regelmæssigt.	Vi har ved vores test konstateret at den implementerede logning ikke stemmer overens med best practice for administrator- og operatørlogning. Vi har ikke konstateret yderligere væsentlige afvigelser.
12.4.4	**Tidssynkronisering** Urene for alle relevante informationsbehandlingssystemer inden for en organisation eller sikkerhedsdomæne skal synkroniseres til en enkelt referencetidskilde.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har inspiceret, at Cloud Factory har etableret en referencetidskilde til klokkesynkronisering af alle relevante informationsbehandlingssystemer.	Vi har ved vores test konstateret at en af de primære switches ikke er konfigureret med tidssynkronisering. Vi har ikke konstateret yderligere væsentlige afvigelser.

A.12 Kontrolmål: Driftsikkerhed

Formål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter og beskytte mod tab af data

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
12.5.1	**Softwareinstallation på driftssystemer** Der skal implementeres procedurer for at kontrollere installationen af software på driftssystemer.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Ved hjælp af stikprøver fra de systemer, der er brugt til at dokumentere ændringer, har vi undersøgt, om – i overensstemmelse med retningslinjer – ændringer i driftsmiljøet udføres ved hjælp af en kontrolleret proces, herunder om: • der udføres en godkendt test før ændringerne implementeres • testning. og godkendelse af nødændringer i driftsmiljøet dokumenteres umiddelbart efter implementering.	Vi har ved vores test konstateret at der ikke er nogen formaliseret procedure eller tekniske foranstaltninger for kontrol af software. Vi har ikke konstateret yderligere væsentlige afvigelser.
12.6.1	**Styring af tekniske sårbarheder** Cloud Factory har defineret procedurer for patch management. Der udføres regelmæssigt test af firewall og dennes evne til at modstå angreb.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for styring af tekniske sårbarheder. Vi har inspiceret proceduren for patch management samt dokumentation for regelmæssig udført test af firewall og dennes evne til at modstå angreb.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.13 kontrolmål: Kommunikationssikkerhed

Formål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
13.1.1	**Netværksstyring** Netværk skal forvaltes og kontrolleres for at beskytte information i systemer og applikationer.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Ved besigtigelse har vi undersøgt, om der – i henhold til retningslinjer – er etableret en passende sikkerhedsarkitektur i netværket, herunder om: • netværket er adskilt i sikre zoner og om kundemiljøer er adskilt fra CloudFactorys eget miljø • fjernadgang er givet gennem to-faktor autentificering • ændringer af netværksmiljøet, der er inkluderet i vores test, er foretaget på en kontrolleret måde i overensstemmelse med ændringsstyringsreglerne.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
13.1.3	**Opdeling af netværk** Grupper af informationstjenester, brugere og informationssystemer skal adskilles på netværk.	Vi har forespurgt om de udførte procedurer/kontrolaktiviteter. Vi har gennemgået den tekniske sikkerhedsarkitektur og har ved kontrol af stikprøver undersøgt, om der – i henhold til retningslinjer – er etableret et passende sikkerhedsniveau, herunder om: • sikre zoner og kundemiljøer er adskilt fra Cloud Factory eget miljø • adgangen til netværket er adskilt i relevante brugergrupper baseret på brugernes arbejdsrelaterede behov.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.15 kontrolmål: Leverandørforhold

Formål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
15.1.1	**Kontakt til samarbejdspartnere** Cloud Factory har i deres rekrutteringspolitik og i dokumentet for it-sikkerhed defineret krav til informationssikkerhed ved anvendelse af underleverandører. Som udgangspunkt skal eksterne samarbejdspartnere efterleve samme regler som en Cloud Factory-medarbejder, herunder også it-sikkerhedspolitikken. I forbindelse med indgåelse af samarbejdsaftaler gøres underleverandøren opmærksom på dette.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået rekrutteringspolitikken samt it-sikkerhedspolitikken for de fastsatte krav vedrørende efterlevelse af samme regler som en Cloud Factory-medarbejder. Vi har ved inspektion gennemgået kontrakter med leverandører og samarbejdspartnere.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
15.1.2	**Håndtering af sikkerhed i leverandørers aftaler** Cloud Factory har indgået skriftlige aftaler med eksterne underleverandører. Cloud Factory får årligt en 3402-erklæring på ydelser, som leveres af eksterne underleverandører.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for håndtering af sikkerhed i leverandøraftaler. Vi har inspiceret skriftlige aftaler med eksterne underleverandører.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.16 kontrolmål: Styring af informationssikkerhedsbrud

Formål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
16.1.1	**Ansvar og procedurer** Ledelsens ansvar og procedurer skal etableres for at sikre en hurtig, effektiv og velordnet reaktion på informationssikkerhedshændelser.	Vi har inspiceret, at der er implementeret en formel og dokumenteret hændelseshåndteringsproces. Vi har inspiceret, at en formel og dokumenteret hændelseshåndteringsproces er blevet gennemgået og godkendt. Vi har inspiceret, at hændelseshåndteringsprocessen er blevet kommunikeret til medarbejderne. Vi har kontrolleret, at alle hændelser er registreret, at nødvendige handlinger er udført, og at løsningerne er dokumenteret i et hændelsesstyringssystem.	Vi har ved vores test ikke konstateret væsentlige afvigelser.

A.17 kontrolmål: Informationssikkerhedsaspekter ved nød-, bedredskabs- og reetableringsstyring

Formål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
17.1.1	**Planlægning af informationssikkerhedskontinuitet** Organisationen skal fastlægge sine krav til informationssikkerhed og kontinuitet i informationssikkerhedsstyringen i ugunstige situationer, fx under en krise eller katastrofe.	Vi har kontrolleret, at en formel og dokumenteret forretningskontinuitetsplan vedligeholdes, revideres og godkendes årligt. Vi har inspiceret, at der er udført en forretningskonsekvensvurdering for at fastlægge kravene til en forretningskontinuitetsplan. Vi har inspiceret, at underliggende procedurer relateret til forretningskontinuitetsplanen er blevet gennemgået og godkendt af passende personale.	Vi har ved vores test konstateret at beredskabsplanen ikke er gennemgået i perioden. Vi har ikke konstateret yderligere væsentlige afvigelser.
17.1.2	**Implementering af informationssikkerhedskontinuitet** Organisationen skal etablere, dokumentere, implementere og vedligeholde processer, procedurer og kontroller for at sikre det nødvendige niveau af kontinuitet for informationssikkerhed under en ugunstig situation.	Vi har kontrolleret, at de underliggende procedurer er implementeret i organisationen. Vi har ved forespørgsel hos relevant personale fået bekræftet medarbejdernes forståelse for kontrollerne i relation til informationssikkerhedskontinuitet.	Vi har ved vores test ikke konstateret væsentlige afvigelser.
17.1.3	**Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten** Organisationen skal verificere de etablerede og implementerede informationssikkerhedskontinuitetskontroller med jævne mellemrum for at sikre, at de er gyldige og effektive i ugunstige situationer.	Vi har inspiceret, at underliggende procedurer for forretningskontinuiteten bliver gennemgået og opdateret. Vi har inspiceret, at de underliggende procedurer er blevet testet for at sikre, at de er gyldige og effektive i ugunstige situationer.	Vi har konstateret at der ikke er foretaget test af beredskabsplaner i perioden. Vi har ikke konstateret yderligere væsentlige afvigelser.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Svend Pedersen
Kunde
Serienummer: 3ef64cfb-6138-4906-9926-905199d08c53
IP: 46.32.xxx.xxx
2023-05-31 09:31:34 UTC

Jesper Parsberg Madsen
Statsautoriseret revisor
Serienummer: d928e935-d26a-4251-b316-bc64d31db8a2
IP: 87.49.xxx.xxx
2023-05-31 10:42:27 UTC

Penneo dokumentnøgle: VQECG-WADM7-Z7CAY-2HELW-GNA14-DIYQ8