Kontainer A/S
Copenhost A/S (binavn)
Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. april 2021 til 31. marts 2022 i relation til it-drift og hosting-ydelser

Juli 2022

Indholdsfortegnelse

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Kontainer A/S' (Kontainer) it-drift og hosting-ydelser, 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.

Kontainer har anvendt AE Corp NL B.V. (Atlas Edge – tidligere Colt Technology Services A/S), Cibicom A/S og Sentia Denmark A/S som serviceunderleverandører af housing af it-miljøer i perioden. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som AE Corp NL B.V. (Atlas Edge – tidligere Colt Technology Services A/S), Cibicom A/S og Sentia Denmark A/S varetager for Kontainer.

Kontainer bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af Kontainers it-drift og hosting-ydelser, der har behandlet kunders transaktioner i hele perioden fra 1. april 2021 til 31. marts 2022. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til Kontainers it-drift og hosting-ydelser 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 Kontainers it-drift og hosting-ydelsers 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
   - 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 Kontainers it-drift og hosting-ydelser foretaget i perioden fra 1. april 2021 til 31. marts 2022

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til Kontainers it-drift og hosting-ydelser, 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 Kontainers it-drift og hosting-ydelser, 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. april 2021 til 31. marts 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. april 2021 til 31. marts 2022.

København, den 8. juli 2022
Kontainer A/S

Jesper Sandberg
Direktør

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. april 2021 til 31. marts 2022 i relation til it-drift og hosting-ydelser

Til: Kontainer, Kontainers kunder og disses revisorer

Omfang
Vi har fået som opgave at afgive erklæring om Kontainers beskrivelse i afsnit 3 af virksomhedens generelle it-kontroller i relation til Kontainers it-drift og hosting-ydelser, der har behandlet kunders transaktioner i hele perioden fra 1. april 2021 til 31. marts 2022, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Kontainer har anvendt AE Corp NL B.V. (Atlas Edge – tidligere Colt Technology Services A/S), Cibicom A/S og Sentia Denmark A/S som serviceunderleverandører af housing af it-miljøer i perioden. Erklæringen anvender partielmetoden og omfatter ikke kontroller, som AE Corp NL B.V. (Atlas Edge – tidligere Colt Technology Services A/S), Cibicom A/S og Sentia Denmark A/S varetager for Kontainer.

Kontainers ansvar
Kontainer 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.

PricewaterhouseCoopers er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar
Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Kontainers 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 sin it-drift og sine hosting-ydelser 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 hensigtsmæssigheden af de kriterier, som Kontainer 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

Kontainers 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 it-drift og hosting-ydelser, 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 Kontainers it-drift og hosting-ydelser, således som de var udformet og implementeret i hele perioden fra 1. april 2021 til 31. marts 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. april 2021 til 31. marts 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. april 2021 til 31. marts 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 Kontainers it-drift og hosting-ydelser, 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 8 juli 2022
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

Rico Lundager
senior manager

3. Kontainer A/S og Copenhost A/S' beskrivelse af generelle it-kontroller for driftsydelser i Danmark

Indledning – kort om Kontainer A/S og Copenhost A/S

Kontainer A/S (Kontainer) og Copenhost A/S (binavn) leverer, servicerer, overvåger, implementerer og drifter it-løsninger for en række forskellige virksomheder.

Copenhost rådgiver, servicerer, implementerer og drifter it-løsninger med fokus på følgende:

- Vi er leverandør af dedikerede, hostede it-løsninger med 24x7-drift.
- Vi er leverandør af it-infrastrukturprojekter.
- Vi er kvalitetsbevidste – leverer altid efter "best practice".
- Vi har speciale i løsninger baseret på Linux-baserede open source-løsninger.
- Alle kunder er unikke for Kontainer.

De etablerede kontroller og procedurer er etableret med afsæt i standarderne ISO 27001/2.

Beskrivelse af ydelser

Kontainers primære ydelser er følgende:

- Levering af Kontainer Billedarkiv
- Levering af dedikerede, hostede services og servere
- Levering af domænehåndtering og delte webhoteller
- Levering af skræddersyede webservere primært baseret på Linux
- Microsoft Exchange
- Kvalificeret support af hosting-ydelser.

Kontainer er co-located i to datacentre, Colt i København S og Sentia i Glostrup, der ligger med ca. 15 kilometers afstand. Herfra foretages al drift af ovennævnte ydelser.

Kontainer har 24/7-overvågning af alle services med fysisk bemanding fra 8 til 17 på hverdage. Resten af tiden er via telefonvagt og alarmer til vagt.

Beskrivelsen omfatter drift og overvågning for perioden 1. april 2021 til 31. marts 2022 og er udelukkende udarbejdet til brug for de virksomheder, der anvender Kontainers it-drift og hosting-aktiviteter, og disse virksomheders revisorer og må ikke anvendes til andre formål.

Ændringer i revisionsperioden

Der er i revisionsperioden foretaget et skift af sekundært hosting-center til Cibicoms helt nye datacenter i Ballerup.

Underleverandører

AtlasEdge Data Centers A/S
Borgmester Christiansens Gade 55
2450 København SV

Cibicom A/S
Industriparken 35-37
2750 Ballerup

Sentia Danmark A/S
Smedeland 32
2600 Glostrup

Kontrolmiljø

Kontainer ledes af Jesper Sandberg.

Supportteamets primære funktion er at levere teknisk support af de hostede løsninger samt mailsupport til slutbrugere.

Hosting-teamets primære funktion er at sikre stabil drift og maksimal oppetid samt at håndtere planlagte servicevinduer på infrastrukturen i datacentrene. Teamet håndterer også overvågning af servere, netværk, storage samt WAN-forbindelse, herunder VPN til kunder. Sidst men ikke mindst håndteres licensrapportering af hosting-teamet. Teamet står også for opsætning af nye kunder, installation af software samt projektstyring af de enkelte nye opgaver.

I Kontainer foretages den interne administrative sikkerhedsfunktion af ledelsen. Ansvaret for den tekniske sikkerhed er placeret i linjeorganisationen. Funktionen sikrer implementering og ajourføring af sikkerheds- og kvalitetsprocedurer, forestår den primære kontakt til revisorer/auditorer, sikrer udførelse af egenkontroller, sikrer løbede vedligeholdelse af risikovurderingen samt sikrer, at der findes en beredskabsplan, og at denne bliver løbende ajourført.

Ansvaret for sikkerhedspolitik, beredskabsplaner, driftsrutiner og beskrivelse af forretningsgang ligger hos ledelsen. Ansvaret for formidling af forretningsgang og interne rutiner ligger hos ledelsen. Ved opdatering/rettelser er det ledelsens ansvar at formidle disse.

Alle operationer kontrolleres løbende via reviews af alle udførte operationer.

Risikostyring

Ledelsen i Kontainer foretager løbende en risikovurdering. Formålet med denne risikovurdering er at identificere og vurdere et passende niveau for risiko af de forskellige dele af driften.

Overvågning

Ledelsen har ansvaret for at overvåge sikkerhedsbrister samt følge op på disse. Det er endvidere ledelsen, der igangsætter udbedring af eventuelle sikkerhedsbrister. Det er medarbejderens ansvar at rapportere sikkerhedsbrister eller mistanke herom til ledelsen omgående.

Kontrolaktiviteter

Der er etableret kontroller, inden for de kontrolmål som fremgår nedenfor. De enkelte kontroller beskrives yderligere i afsnit 4.

- Skriftlig politik for informationssikkerhed
- Organisering af informationssikkerhed
- Fysisk sikkerhed
- Styring af kommunikation og drift
- Adgangsstyring
- Anskaffelse, udvikling og vedligeholdelse af styresystemer
- Katastrofeplan.

Komplementerende kontroller

Forudsætninger vedrørende kundernes ansvar er beskrevet i individuelle kontrakter. Kunden er ansvarlig for egne data. Det betyder, at kunden er ansvarlig for de ændringer, der måtte foretages i data, når der er logget på systemet med individuelle brugernavne og adgangskoder. Ved tredjepartsadgang bestilt af kunden er det kunden, som har ansvaret for opfølgning på kontrollen.

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. april 2021 til 31. marts 2022. Dette omfatter bl.a. vurdering af patching-niveau, tilladte services, segmentering, passwordkompleksitet mv. samt besigtigelse af 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

Kontrolmål A: Informationssikkerhedspolitik

Ledelsen har udarbejdet en informationssikkerhedspolitik, som udstikker en klar målsætning for it-sikkerhed, herunder valg af referenceramme samt tildeling af ressourcer. Informationssikkerhedspolitikken vedligeholdes under hensyn til en aktuel risikovurdering.

Kontrolmål/kontrol	PwC-test	Resultat af test
Skriftlig politik for informationssikkerhed Kontainer A/S har udarbejdet en sikkerhedspolitik. Denne er til rådighed for medarbejderne på fællesdrev. Den revideres mindst én gang årlig. Den er godkendt af ledelsen.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har endvidere inspiceret, at ledelsen har godkendt sikkerhedspolitikken, samt at den som minimum er revurderet én gang årligt. Endvidere har vi inspiceret, at den forefindes let tilgængelig for medarbejderne.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål B: Organisering af informationssikkerhed

Det organisatoriske ansvar for informationssikkerhed er passende dokumenteret og implementeret, ligesom håndtering af eksterne parter sikrer en tilstrækkelig behandling af sikkerhed i aftaler.

Kontrolmål/kontrol	PwC-test	Resultat af test
Ledelsens forpligtelse til informationssikkerhed Den enkelte afdelingsleder er ansvarlig for, at nye medarbejdere gøres bekendt med retningslinjerne som en del af introduktionen til virksomheden. I takt med at der sker opdatering af retningslinjerne, vil der blive givet besked herom via mail og på fællesdrev, hvor man også kan finde den ajourførte og gældende version af sikkerhedspolitikken. Der er løbende fokus på at sikre de rette ressourcer – internt eller eksternt – til at varetage de rette opgaver med rette kompetencer.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har inspiceret, at det organisatoriske ansvar for informations-sikkerhed er dokumenteret og implementeret via en sikkerhedspolitik. Vi har inspiceret, at der er udarbejdet en sikkerhedshåndbog, der beskriver væsentlige retningslinjer for organisationen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Eksterne parter Kontainer A/S beder samarbejdspartnere og eksterne leverandører om at sende revisorerklæring vedrørende de aftalte serviceydelser eller underskrive en kontrakt, der beskriver fortrolighed og sikkerhedsforanstaltninger. Kontainer A/S sikrer, at eksterne partnere er bekendt med Kontainer A/S' sikkerhedspolitik.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er etableret betryggende procedurer for samarbejde med eksterne leverandører. Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte aftaler. Vi har inspiceret, at der er modtaget ISO 27001-certifikat fra housing-leverandøren AE Corp NL B.V og revisionserklæring fra housing-leverandøren Cibicom A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader forårsaget af fysiske forhold som fx brand, vand, strømafbrydelse, tyveri eller hærværk.

Kontrolmål/kontrol	PwC-test	Resultat af test
Fysisk sikkerhedsafgrænsning Kontainer A/S anvender housing-leverandørerne AE Corp NL B.V. og Cibicom A/S. Kontainer A/S modtager årligt et ISO 27001-certifikat fra AE Corp NL B.V. og en ISAE 3402 type 2-revisionserklæring fra Cibicom A/S. Alle medarbejdere hos Kontainer A/S har adgang til kontorlokalerne i city ved hjælp af nøgle.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er modtaget ISO 27001-certifikat fra housing-leverandøren AE Corp NL B.V og revisionserklæring fra housing-leverandøren Cibicom A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Sikring af kontorer, lokaler og faciliteter Kontainer A/S anvender housing-leverandørerne AE Corp NL B.V. og Cibicom A/S. Kontainer A/S modtager årligt et ISO 27001-certifikat fra AE Corp NL B.V. og en ISAE 3402 type 2-revisionserklæring fra Cibicom A/S. Alle medarbejdere hos Kontainer A/S har adgang til kontorlokalerne i city ved hjælp af nøgle.	Vi har forespurgt ledelsen om anvendte procedurer. Vi har inspiceret, at der er modtaget ISO 27001-certifikat fra housing-leverandøren AE Corp NL B.V og revisionserklæring fra housing-leverandøren Cibicom A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Placering og beskyttelse af udstyr Kontainer A/S anvender housing-leverandørerne AE Corp NL B.V. og Cibicom A/S. Kontainer A/S modtager årligt et ISO 27001-certifikat fra AE Corp NL B.V. og en ISAE 3402 type 2-revisionserklæring fra Cibicom A/S.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er modtaget ISO 27001-certifikat fra housing-leverandøren AE Corp NL B.V og revisionserklæring fra housing-leverandøren Cibicom A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Understøttende forsyninger (forsyningssikkerhed) Kontainer A/S anvender housing-leverandørerne AE Corp NL B.V. og Cibicom A/S. Kontainer A/S modtager årligt et ISO 27001-certifikat fra AE Corp NL B.V. og en ISAE 3402 type 2-revisionserklæring fra Cibicom A/S.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at der er modtaget ISO 27001-certifikat fra housing-leverandøren AE Corp NL B.V og revisionserklæring fra housing-leverandøren Cibicom A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål C: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader forårsaget af fysiske forhold som fx brand, vand, strømafbrydelse, tyveri eller hærværk.

Kontrolmål/kontrol	PwC-test	Resultat af test
Sikring af kabler Kontainer A/S anvender housing-leverandørerne AE Corp NL B.V. og Cibicom A/S. Kontainer A/S modtager årligt et ISO 27001-certifikat fra AE Corp NL B.V. og en ISAE 3402 type 2-revisionserklæring fra Cibicom A/S. Krydsfeltet i kontorlokalerne i city er forsvarligt aflåst.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har observeret ved inspektion, at krydsfeltet på kontoret er forsvarligt aflåst. Vi har inspiceret, at der er modtaget ISO 27001-certifikat fra housing-leverandøren AE Corp NL B.V og revisionserklæring fra housing-leverandøren Cibicom A/S.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder overvågning, registrering og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift og brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed og fortrolighed.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Dokumenterede driftsprocedurer Kontainer A/S har beskrevet driftsprocedurerne for driftsmiljøet. Kontainer A/S har to forskellige typer medarbejdere; support og drift. Opgaver med storage, firewall og adgangskontrol hører til under drift. Kontainer A/S har ingen udviklings- eller applikationsvedligehold.	Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenteret. I forbindelse med revisionen af de enkelte driftsområder er det ved inspektion kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Foranstaltninger mod virus og lignende skadelig kode Der er installeret antivirusprogrammer, som bliver opdateret regelmæssigt. Kontainer A/S benytter anerkendt værktøj til antivirus med automatisk versionskontrol.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspiceret den tekniske opsætning til bekræftelse af, at der er installeret antivirusprogrammer, samt at disse er opdateret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Sikkerhedskopiering af informationer Backup og validering foretages. Der benyttes Veeam til backup/restore af virtuelle servere. Veeam benyttes også som disaster recovery backup. Der udføres periodisk restore-test af servere og data.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, inspiceret backupprocedurer samt inspiceret, at de er tilstrækkelige og formelt dokumenteret. Vi har ved stikprøvevis inspiceret log vedrørende backup til bekræftelse af, at backupper er gennemført fejlfrit, alternativt at der foretages afhjælpning i tilfælde af mislykkede backupper. Vi har ved stikprøvevis inspiceret, at restore af servere er gennemført succesfuldt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål D: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder overvågning, registrering og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for sikkerhedskopiering og beredskabsplaner*
- *passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift og brugerfunktioner*
- *passende forretningsgange og kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed og fortrolighed.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Monitorering af systemanvendelse og auditlogning Der er implementeret logning ved adgang på kritiske systemer. Disse logge bliver gennemgået i tilfælde af mistanke om misbrug eller fejl. Alle brugeres rettigheder bliver kontrolleret mindst to gang om året eller ved til-/afgang af medarbejdere. Alt hardware er overvåget. Der afsendes rapport i tilfælde af fejl. Overvågningssystem sender sms og mail i tilfælde af fejl.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, inspiceret systemopsætningen på servere og væsentlige netværksenheder samt inspiceret, at parametre for logning er opsat, således at handlinger udført af brugere med udvidede rettigheder bliver logget. Vi har ved stikprøvevis inspiceret, at der er etableret overvågning og alarmering for nedsat tilgængelighed samt for forsøg på brud på den etablerede sikkerheds-foranstaltning. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at der foretages tilstrækkelig opfølgning på logge fra kritiske systemer.	Vi har under vores revision af domain controller observeret, at auditloggen ikke er konfigureret tilstrækkeligt. Vi har efterfølgende fået oplyst, at konfiguration af logning er ændret. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.
Administrator- og operatørlog Kontainer A/S logger transaktioner og handlinger, der er gennemført af brugere og administratorer via domain controllers (AD) auditlog og Linux syslog til Graylog. Brugerkontis rettigheder på AD og Ipa gennemgås halvårligt. Logge fra AD og Graylog og andre væsentlige systemer bliver gennemgået løbende og ved begrundet mistanke om uautoriserede handlinger.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret systemopsætningen på servere og væsentlige netværksenheder samt inspiceret, at parametrene for logning er opsat, således at handlinger udført af brugere med udvidede rettigheder bliver logget. Vi har endvidere stikprøvevist kontrolleret, at der foretages tilstrækkelig opfølgning på logge fra kritiske systemer.	Se "Monitorering af systemanvendelse og auditlogning" ovenfor. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Brugerregistrering og administration af privilegier Oprettelse og nedlæggelse af brugere er ledelsesgruppens (LG) ansvar. Brugerne oprettes i forhold til et arbejdsbetinget behov. Proceduren er godkendt af ledelsen. Adgang til kundernes systemer er kundens ansvar. Derfor har Kontainer A/S ikke beskrevet dette. Brugere oprettes i grupper. Det er disse grupper, der har rettighederne til, hvad den enkelte medarbejder har adgang til. Det er LG, der beslutter, hvilke grupper en medarbejder skal være medlem af. LG vurderer løbende, om Kontainer A/S' medarbejdere har de rigtige rettigheder. Samtlige brugere i Kontainer A/S' AD og disses rettigheder bliver gennemgået minimum to gange årligt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspiceret, at det er LG, der godkender tildeling af adgang til systemerne, samt stikprøvevist kontrolleret, at forretningsgangene er overholdt for oprettede brugere på Kontainer A/S' systemer. Vi har foretaget stikprøvevis kontrol af, at halvårlige gennemgange foretages.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Administration af brugeradgangskoder (passwords) Der er implementeret programmerede kontroller, der sikrer, at passwords har den fornødne kvalitet, jf. sikkerhedspolitikkens bestemmelser. Passwords skal bestå af minimum otte tegn, og tegnene skal være en blanding af tal og bogstaver. Passwords er gyldige i maks. 90 dage og kan ikke genbruges.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordkontroller, og inspiceret, at det sikres, at der anvendes passende autentifikation af brugere på alle adgangsveje. Vi har ved inspektion kontrolleret, at der anvendes en passende passwordkvalitet i Kontainer A/S' driftsmiljø ved stikprøvevise test af, at adgang til virksomhedens systemer sker ved brug af brugernavn og password.	Vi har under vores revision af udvalgte kunderelaterede Windows-servere observeret, at password-politikken ikke er konfigureret tilstrækkeligt på to servere. Vi er efterfølgende blevet informeret om, at Kontainer A/S har ændret passwordpolitik på de pågældende servere. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Evaluering af brugeradgangsrettigheder Kontainer A/S foretager periodisk review af brugerrettigheder to gange årligt, til sikring af at disse er i overensstemmelse med brugernes arbejdsbetingede behov. Uoverensstemmelser undersøges og rettes rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion kontrolleret, at der foretages periodiske gennemgange til bekræftelse af, at disse har fundet sted, samt inspiceret, at identificerede afvigelser afhjælpes.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Inddragelse af adgangsrettigheder Brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver deaktiveret ved disse medarbejderes fratrædelse. Ledelsen godkender inddragelse af rettigheder og nedlæggelse af brugere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at inddragelse af adgangsrettigheder sker efter betryggende forretningsgange, og at der foretages opfølgning i henhold til forretningsgangene på de tildelte adgangsrettigheder. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugere på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Styring af netværksforbindelser Kundernes netværk er adskilt via firewallfiltre. Kontainer A/S gennemgår periodisk firewallregler for at sikre mod uautoriseret adgang. Som udgangspunkt er der lukket for trafik udefra. Ønsker kunderne dette ændret, sker dette efter skriftlig anmodning. Der skal være DDOS-filter på forbindelser til datacenteret. Logge fra firewallen gemmes på ekstern logserver i min. 60 dage.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret, at netværket er delt op i adskilte VLAN'er, at der er etableret personhenførbare brugerkonti i firewallen, samt at der udarbejdes behørig dokumentation for reglerne. Vi har inspiceret, at der er implementeret deep packet inspection-firewall, og har ved stikprøvevis inspiceret regler. Vi har inspiceret, at der er indgået aftale med leverandøren af DDOS-løsningen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål E: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data*
- *fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Kontrolmål/kontrol	PwC-test	Resultat af test
Begrænset adgang til informationer Kun personer med behov for adgang til kundespecifikke systemer har adgang. Alle adgangsønsker for nye og eksisterende brugere vedrørende applikationer, databaser og datafiler bliver gennemgået for at sikre overensstemmelse med Kontainer A/S' politikker, til sikring af at rettigheder tildeles ud fra et arbejdsbetinget behov, er godkendt samt bliver korrekt oprettet i systemer.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at begrænse adgangen til informationer. Vi har inspiceret procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteterne er tilstrækkeligt dækkende. Vi har ved stikprøvevis inspektion kontrolleret, at tildeling af adgang til data og systemer udføres ud fra et arbejdsbetinget behov og er godkendt i overensstemmelse med forretningsgangene.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

Der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

Kontrolmål/kontrol	PwC-test	Resultat af test
Styring af software på driftssystemer It-miljøet for kundernes systemer er adskilt fra andre kunder samt det interne Kontainer A/S-it-miljø. For de kunder, hvor det er aftalt, findes der separate udviklings-, test- og produktionsmiljøer. Kontainer A/S benytter patch management til at styre fx OS-opgraderingen. Patching af kundeservere aftales og accepteres i samarbejde med den enkelte kunde. Patching udføres i aftalt servicevindue. Proceduren omfatter både OS og applikationer, så længe applikationer kan indgå i Kontainer A/S' repositories.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at adskillelse mellem enkelte miljøer opretholdes. Desuden har vi forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at holde kritiske systemer opdaterede og gennemgåede, samt opdateringsprocedurernes tilstrækkelighed, hvad angår Kontainer A/S' egne væsentlige systemer og kundernes systemer i henhold til kontraktlige aftaler. Vi har ved stikprøvevis inspiceret ændringer i perioden og har inspiceret, at ændringerne er dokumenteret. Vi har endvidere stikprøvevis efterprøvet kontrollerne, herunder at: • der er tilstrækkelig kommunikation med leverandørerne med henblik på at modtage nødvendige informationer om kritiske og vigtige opdateringer, samt at der foretages de fornødne risikovurderinger af de enkelte opdateringer • de kritiske systemer er blevet opdateret hensigtsmæssigt.	Vores test har ikke konstateret væsentlige afvigelser.

Kontrolmål F: Anskaffelse, udvikling og vedligeholdelse af styresystemer

Der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse af styresystemer.

Kontrolmål/kontrol	PwC-test	Resultat af test
Ændringsstyring Kontainer A/S bruger change management til at styre ændringer. Ændringer af daglige arbejdsopgaver er beskrevet i standard change, som er forhåndsgodkendt. Ingen ændringer i produktion implementeres, før change er godkendt af kunden og ledelsen samt testet, og fallback-plan er udformet. Nødændringer uden om den normale forretningsgang testes og godkendes efterfølgende. Ingen ændring må udføres uden godkendelse.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og inspiceret change management-procedurernes tilstrækkelighed samt inspiceret, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur. Vi har ved stikprøvevis inspiceret ændringsønsker for følgende: • Registrering af ændringsanmodninger i det dertil etablerede system • Dokumenteret test af ændringer, herunder godkendelse • Godkendelse skal være opnået før implementering Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende • Dokumenteret plan for tilbagerulning, hvor relevant.	Vi har under vores revision af ændringsstyring observeret, at ændringerne ikke bliver prioriteret i overensstemmelse med ændringskategorierne som definerer hvorvidt ændringerne skal være underlagt godkendelse, test og fallbackplaner. Vi har ikke ved vores test konstateret yderligere væsentlige afvigelser.

Kontrolmål G: Katastrofeplan

Kontainer A/S er i stand til at fortsætte servicering af sine kunder i en katastrofesituation.

Kontrolmål/kontrol	PwC-test	Resultat af test
Opbygning/struktur af katastrofeberedskab Kontainer A/S har udarbejdet en katastrofeplan. Denne beskriver sandsynligheder samt de nødvendige tiltag. Planen er godkendt af ledelsen og revideres årligt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har inspiceret udleveret materiale vedrørende katastrofeberedskab samt inspiceret, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Test af katastrofeberedskab Der sker årlig test af katastrofeberedskabet ved såvel skrivebordstest som faktiske testscenarier. Såfremt testen afslører uhensigtsmæssigheder, opdateres planen umiddelbart herefter.	Vi har ved stikprøvevis inspektion kontrolleret, at beredskabsplanerne testes ved skrivebordstest eller via realistiske testscenarier, i det omfang det er muligt.	Vi har ikke ved vores test konstateret 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."

Jesper Sandberg Bentel
Direktør
På vegne af: Kontainer A/S
Serienummer: PID:9208-2002-2-029222017562
IP: 212.60.xxx.xxx
2022-07-08 08:24:33 UTC
NEM ID

Jesper Parsberg Madsen
Statsautoriseret revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: PID:9208-2002-2-427963640472
IP: 83.136.xxx.xxx
2022-07-08 08:40:44 UTC
NEM ID

Rico Lundager
Revisor
På vegne af: PricewaterhouseCoopers Statsautoriseret…
Serienummer: CVR:33771231-RID:30016557
IP: 83.136.xxx.xxx
2022-07-08 08:51:47 UTC
NEM ID