Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med hosting-ydelsen i perioden 01-12-2016 til 30-11-2017

ISAE 3402-II

any.cloud A/S

CVR-nr.: 31 16 15 09

december 2017

Indholdsfortegnelse

Afsnit 1: any.cloud A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt any.cloud A/S' hosting-ydelse, 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. any.cloud A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af any.cloud A/S' hosting-ydelse til kunder i hele perioden fra 01-12-2016 til 30-11-2017. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan systemet var udformet og implementeret, herunder redegør for:

- De typer af ydelser, der er leveret, når det er relevant
- De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
- Relevante kontrolmål og kontroller, udformet til at nå disse mål
- Kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner.

(ii) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 01-12-2016 til 30-11-2017

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

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra 01-12-2016 til 30-11-2017. Kriterierne for denne udtalelse var, at:

(i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificerede

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 01-12-2016 til 30-11-2017.

København, 19. december 2017
any.cloud A/S

Gregor Møller
CEO

Afsnit 2: any.cloud A/S' beskrivelse af kontroller i forbindelse med drift af deres hosting-ydelse

Beskrivelse af kontrolmiljø for hostingmiljø

Introduktion

Formålet med denne beskrivelse er at levere information til any.cloud A/S' kunder og deres revisorer vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402.

Beskrivelsen har herudover det formål at give information om de kontroller, der er anvendt for cloud-tjenester hos os i perioden.

Beskrivelsen omfatter de kontrolmål og kontroller hos any.cloud, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold er ikke medtaget i denne beskrivelse.

any.cloud

Formålet med denne beskrivelse er at levere information til any.cloud A/S' kunder og deres revisorer vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402.

Beskrivelsen har herudover det formål at give information om de kontroller, der er anvendt for serviceydelser hos os i perioden.

Beskrivelsen omfatter de kontrolmål og kontroller hos any.cloud, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold er ikke medtaget i denne beskrivelse.

any.cloud leverer professionelle ISO-certificerede hosting- og rådgivningsservices samt on-site- support og IT-drift og salg af hardware og software til dansk erhvervsliv.

any.clouds væsentligste aktivitet er levering af services, herunder:

- PaaS - VPS (Virtual Private Server)
- BaaS & DRaaS - virtual backup med DRS (Disaster Recovery Solution)
- Netværkssikkerhed, herunder DDoS og hacking
- MPLS- og fiberinfrastruktur
- Rådgivning, support og drift af IT-installationer
- Salg og leasing af hardware og software.

Vi leverer højeste kvalitet af IT-løsninger, IT-support og infrastruktur igennem de bedste leverandører og præsenterer dette til vores kunder via simple og innovative løsninger.

Vi yder en stor indsats for at få komplicerede services gjort enkle for vores kunder samt både proaktivt og efter opstået behov at håndtere de udfordringer, som de måtte møde i deres daglige omgang med IT. Det er vores mål, at kunden kan fokusere på sin forretning. Vi supporterer og drifter IT for virksomheder og deres ansatte og sørger for, at de altid kan arbejde - sikkert, effektivt og til en meget fordelagtig pris.

any.cloud har en ISAE 3402 Type II-revisorerklæring og arbejder under ISO27002-standarden. Dette sikrer, at vi konstant opretholder den kvalitet, det kræver for at tilhøre den absolutte elite inden for IT-løsninger.

any.clouds infrastruktur er hostet i InterXion Danmark i Ballerup og Global Connect i Tåstrup, som begge er europæisk udbydere af cloud- og operatørneutrale datacentre med over 48 datacentre fordelt på 11 lande. any.cloud har yderligere hostingservices i det 35 datacenter store IBM-ejede selskab Softlayer og leverer herigennem produkter i hele verden.

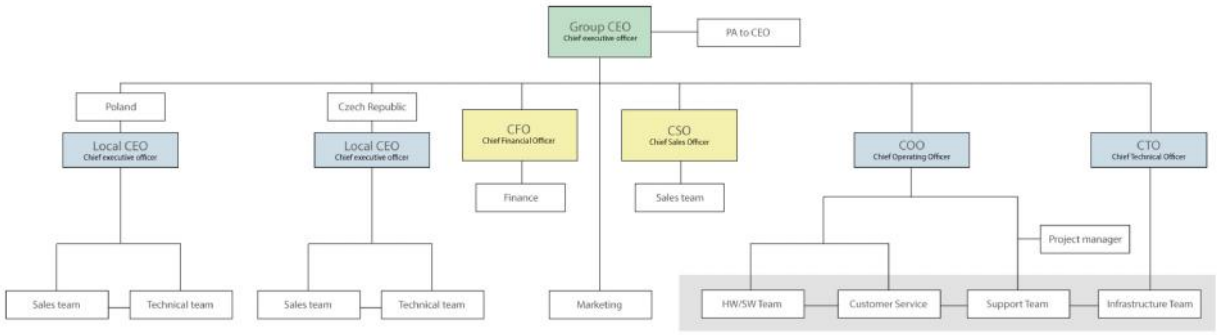
any.cloud er bl.a. med sine recertificeringer af hostingcertifikatet fra BFIH en del af Danmarks bedste hostere. Som kontinuerligt certificeret medlem og med opnåelse af hostingmærket er any.cloud forpligtet til at levere under hensyntagen til strenge kontrolforanstaltninger, høje sikkerhedskrav samt gennemsigtighed i forhold til indhold af kvalitet og sikkerhed i IT-hostingydelser.

Vi er et stærkt hold med både kontorer og medarbejdere i Danmark, Polen og Tjekkiet.

any.cloud – RESHAPE THE FUTURE

Organisation og ansvar

any.cloud har en klar og gennemsigtig virksomhedsstruktur.



any.cloud beskæftiger 36 medarbejdere og er inddelt i tre business units: Support Team, Infrastructure Team og HW/SW Team.

Risikovurdering og -håndtering

Risikovurdering

IT-risikoanalyse

Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores cloud tjenester. Dermed kan vi sikre, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau.

Risikovurdering foretages periodisk samt, når vi foretager ændringer eller implementerer nye systemer, som vi vurderer at være relevante til at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderinger er hos virksomhedens CTO og skal efterfølgende forankres og godkendes hos ledelsen.

Håndtering af sikkerhedsrisici

Procedure for risikohåndtering
Vi har indført pointsystem på de risici, der er forbundet med levering af cloud ydelser. Vi bruger beregningsformen risiko*påvirkning med en score fra 1-10. Det acceptable niveau går til 30 point. Det tages løbende op til vurdering om hvorvidt vi kan nedbringe risici og lave tiltag, der kan forbedre vores score.

Sikkerhedspolitik

IT-sikkerhedspolitik

IT-sikkerhedspolitik-dokument
Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere stabil og sikker hosting-drift til vores kunder. For at kunne gøre dette, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartet og gennemsigtige.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27002 (Regelsæt for styring af informationssikkerhed), og er dermed helt overordnet inddelt i følgende kontrolområder:

- Organisation og ansvar
- Medarbejdersikkerhed
- Logisk adgangsstyring
- Risikovurdering og håndtering
- Fysisk sikkerhed
- Brug af it-udstyr
- Driftsafviklingsprocedurer
- Netværket
- Support
- Beskyttelse mod ondsindet programmel
- Anskaffelse og vedligeholdelse af systemer
- Samarbejdspartnere, herunder:
  - IBM Softlayer
  - Microsoft Azure
- Beredskabsplanlægning

Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

Vi er medlem af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), og vi bliver i den forbindelse årligt revideret for hvorvidt, vi lever op til BFIH's regelsæt, der centrerer sig om hvordan vi leverer vores driftsydelser, foretager genetablering, håndterer sikkerhedsopdatering mv.

Evaluering af it-sikkerhedspolitikken
Vi opdaterer løbende it-sikkerhedspolitikken, og som minimum én gang årligt.

Organisering af informationssikkerhed

Intern organisering

Delegering af ansvar for informationssikkerhed
Vi har en klart opdelt organisation hvad angår ansvar, og har udførlige ansvars- og rollebeskrivelser på alle niveauer lige fra ledelsesniveau til de enkelte driftsmedarbejdere.

Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter.

Funktionsadskillelse
Gennem løbende dokumentation og processer sikrer vi at kunne udelukke eller minimere nøglepersonsafhængighed. Opgaver tildeles og fastsættes via procedurer for styring af den operative drift.

Kontakt med særlige interessegrupper
Vi har etableret kontakt til hotline hos DK-CERT, hvor vi gensidigt har aftale om orientering ved væsentlige sikkerhedsrelaterede forhold vedrørende internettrafik.

Informationssikkerhed som en del af projektstyring
Såfremt at vi vurderer at et projekt ikke overholder vores informationssikkerhed, vil projektet enten blive tilrettet således at dette efterfølgende overholder vores standard indenfor informationssikkerhed. Vurderer vi at projektet slet ikke kan udføres eller ændres uden at stride imod vores sikkerhedspolitik, vil projektet blive kasseret.

Mobilt udstyr og fjernarbejdspladser

Mobilt udstyr og kommunikation
Vi har etableret mulighed for, at vores medarbejdere kan arbejde hjemmefra af hensyn til bl.a. driftsvagt, og vi har politik for, at udstyr (bærbare mv.) ikke benyttes til andet end arbejdsrelaterede forhold og ikke efterlades uden opsyn mv. Bærbare enheder er sikret med logon, og kryptering.

Vi har åbnet adgang til, at vi og vores kunder kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Ud over kode, har vi 2-factor slået til for forbedret sikkerhed.

Vores kunder har mulighed for samme, og det er op til vores kunder at implementere deres sikkerhedspolitik for deres brugere.

Fjernarbejdspladser
Adgang til vores netværk og dermed potentielt til systemer og data sker kun for autoriserede personer. Vores medarbejdere har adgang via fjernarbejdspladser hvor der anvendes VPN til RDS. 2-factor beskyttelse benyttes altid hvis der kobles op udefra.

Sikkerhed i forhold til HR

Inden ansættelse

Screening
Vi har procedurer for ansættelse af medarbejdere og etablering af samarbejde med eksterne, hvor vi sikrer, at vi ansætter den rigtige kandidat i forhold til baggrund og kompetence. Vi har rolle- og ansvarsbeskrivelser for medarbejdere og medarbejderkategorier, så alle er bekendte med deres ansvar. Alle medarbejdere bliver ved ansættelse gennemgået og et oprettelsesskema følges.

Ansættelsesforhold

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet.

Under ansættelse

Ledelsens ansvar

I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. ligeledes er det klart defineret som en del af kontraktmaterialet, hvad den ansattes ansvar og rolle er.

Bevidsthed om, uddannelse og træning i informationssikkerhed

Vores aktiver er i høj grad vores medarbejdere, og vi fører en struktureret metodik i forhold til vores medarbejderes kvalifikationer, uddannelse og certificeringer. Der afholdes løbende, dog minimum årligt, kurser, foredrag samt andre relevante aktiviteter til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med sikkerhed og bevidstgøres om evt. nye trusler. Medarbejdere, og eksterne parter, hvor det er relevant at inkludere disse under vores sikkerhedsretningslinjer, bliver periodisk orienteret om vores sikkerhedsretningslinjer samt, når der sker ændringer.

Sanktioner

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet.

Ansvar ved ophør

Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm, samt sikre at alle medarbejderes adgange til bygninger, systemer og data inddrages. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos virksomhedens CTO.

Styring af aktiver

Ansvar for aktiver

Fortegnelse over aktiver

Software, servere og netværksudstyr inkl. konfiguration er registreret til brug ved dokumentation, overblik over udstyr mv. Vores netværk er komplekst med mange systemer og kunder, og for at sikre mod uvedkommendes adgang, og for at sikre gennemskueligheden af opbygningen, har vi udformet dokumentation, der beskriver det interne netværk med enheder, navngivning af enheder, logisk opdeling af netværk mv.

Dokumenterne, netværkstopologier og lignende opdateres løbende ved ændringer og gennemgås minimum årligt af vores netværksspecialister.

Ejerskab af aktiver

Via ansvarsfordeling og rollebeskrivelser, er centrale netværksenheder, servere, periferienheder, systemer og data tilegnet systemansvarlige i vores virksomhed. Kunders data og systemer er tilegnet kundens kontaktperson.

Acceptabel brug af aktiver

Dette er beskrevet i medarbejderhåndbogen.

Tilbagelevering af aktiver

Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm, samt sikre at alle medarbejderes adgange til bygninger, systemer og data inddrages. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos virksomhedens CTO.

Mediehåndtering

Styring af bærbare medier

Vi sikrer, i bedst muligt omfang, at vores medarbejderes bærbare medier såsom bærbar pc, mobiltelefon og lignende er konfigureret sikkerhedsmæssigt lige så højt, som resten af vores miljø, samt det sikres, at de databærende medier opdateres, når vi foretager nye sikkerhedstiltag.

Adgangskontrol

Forretningskrav til adgangskontrol

Politikker for adgangsstyring

Vi har politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik.

Administration af brugeradgange

Brugeroprettelses- og nedlæggelsesprocedurer

Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores kunder er dermed ansvarlige for oprettelse og nedlæggelse af brugerkonti.

Alle brugere skal være personhenførbare, dvs. have tydeligt mærke med personnavn. Er der tale om servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret.

Rettighedstildeling

Tildeling af privilegier er kontrolleret i forbindelse med vores normale brugeradministrationsproces.

Håndtering af fortrolige logon informationer

Alle personlige logons er udelukkende kendt af medarbejderen og underlagt passwordpolitik til sikring af kompleksitet.

Evaluering af brugeradgangsrettigheder

For vores egne brugere, gennemgår virksomhedens CTO periodisk, minimum årligt, virksomhedens interne systemer med oprettede brugere og deres adgangsniveau for at sikre mod adgang for uautoriserede personer.

Brugeransvar

Brug af fortrolig adgangskode

Vores it-sikkerhedspolitik beskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet. Medarbejdere skriver årligt under på, at de har læst og forstået seneste version af vores it-sikkerhedspolitik. Da vi har brugere, såsom service accounts og lignende, som ikke kan bruges til at logge på med, og af systemmæssige årsager ikke skifter passwords, har vi et system til opbevaring af disse passwords. Kun autoriseret personale har adgang til systemet.

Kontrol af adgang til systemer og data

Begrænset adgang til data
Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen.

System for administration af adgangskoder
Alle medarbejdere på tværs af både kundesystemer og egne systemer, har restriktioner omkring adgangskode. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger i forhold til udformningen af kodeordet. Koder skal skiftes regelmæssigt og være komplekse.

Vores it-sikkerhedspolitik beskriver regler for kompleksitet samt vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.

Fysiske og miljømæssige sikringer

Vedligeholdelse af udstyr
Datacentrets køle- og brandanlæg bliver efterset periodisk, ligesom nødstrømsanlægget (Dieselgeneratorer & UPS) halvårligt får foretaget eftersyn. Datacentret har opsat systemer således, at der overvåges temperaturer og strømspændinger i serverrummet.

Sikring af udstyr uden for virksomhedens lokaler
Vi fører natligt backupprocedure for sikring af vores kunders data og systemer, såfremt vores hostingsystemer af den ene eller anden årsag bliver utilgængelig.

Vi har en aftale med den pågældende leverandør om housing af vores egne servere, og der er implementeret tilsvarende foranstaltninger mod tyveri, brand, vand og temperaturafvigelser.

Vi modtager årligt revisorerklæring, der afdækker den fysiske sikkerhed hos vores underleverandører.

Senest har vi modtaget revisorerklæringer som dækker perioden 01/01-2016 til 31/12-2016. Erklæringen er afgivet uden forbehold.

Sikker bortskaffelse eller genbrug af udstyr
Alt databærende udstyr destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt.

Brugerudstyr uden opsyn
Alle interne brugerkonti er centralt styret til at gå på skærmlås ved inaktivitet efter max 2 minutter. Dermed sikrer vi, at uautoriseret personale ikke opnår adgang til fortroligt data.

Sikkerhed i forbindelse med drift

Operationelle procedurer og ansvarsområder

Dokumenterede driftsprocedure
Selvom vores organisation ikke nødvendigvis gør, at vi kan have overlap inden for alle opgaver og systemer, sikrer vi via dokumentationer og beskrivelser – og via kompetente og flittige medarbejdere – at medarbejdere eller nye medarbejdere kan påbegynde et arbejde på et system, som vedkommende ikke har operationel og historisk erfaring med. Vi opererer med dobbeltroller på alle systemer således, at den primære ansvarlige medarbejder har ansvar for at kommunikere praktiske forhold til kollegaer. Systemdokumentationen opdateres løbende.

Ændringsstyring

Vi har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder og tilrettelagt hensigtsmæssigt i forhold til interne forhold. Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer. Herudover følges en proces omkring udvikling og test.

Ved alle interne ændring, der er tale om, sikres det altid, som minimum, at;

- Alle ændringer drøftes, prioriteres og godkendes af ledelsen
- Alle ændringer testes
- Alle ændringer godkendes før idriftsættelse
- Alle ændringer idriftsættes på et fastsat tidspunkt efter aftale med forretningen og kunder
- Der fortages fallback-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis den ikke fungerer
- Systemdokumentationen opdateres med den nye ændring, såfremt det vurderes nødvendigt.

Ved standard ændringer behøver risikovurdering ikke at foreligge, ligeledes er godkendelse fra ledelsen heller ikke nødvendig. Dog kræves alle standard ændringer altid kundens accept på skrift.

Vores miljø er adskilt logisk og opdelt i test og produktion, hvorved vi sikre at have testet et produkt, før det kommer i produktion. Via adgangskontroller sikrer vi, at kun autoriseret personale har adgang til dette.

Kapacitetsstyring

Via vores generelle overvågningssystem, har vi sat grænseværdier for hvornår vores overordnede systemer, og dermed vores kunders systemer, skal skaleres op af hensyn til elektronisk plads, svartider mv. Når vi opsætter nye systemer foretages test af funktionalitet og herunder kapacitet- og performancetest. Der er udarbejdet en fast procedure for rapportering af kapacitetsproblemer.

Beskyttelse mod cryptoware, malware & DDoS

Foranstaltninger mod cryptoware, malware & DDoS

Vi har implementeret scannings- og overvågningssystemer til at sikre mod kendt skadevoldende kode, dvs. hvad vi og vores kunder – via vores platforme – kan risikere at blive inficeret med på internettet, via mails mv. Vi har antivirus-systemer, anti-malware på alle platforme, systemer til overvågning af internetbrug, trafik og ressourcer på SaaS platforme, sikringer i øvrige tekniske og centrale installationer (firewall mv.). Ligeledes tilbyder vi anti-DDoS-løsninger til sikring imod DDoS angreb.

Vi har løbende forbedringer af beskyttelse imod nye cryptoware-varianter således at vores data og systemer er beskyttet imod kendte cryptoware-varianter.

Backup

Sikkerhedskopiering af informationer

Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, og efter de aftaler, vi har med vores kunder.

Vi har en test af, hvordan systemer og data praktisk kan retableres. Der føres en log over disse tests således, at vi kan følge op på, om vi kan ændre på procedurer og processer for at højne vores løsning.

Med mindre andet er aftalt med vores kunder, foretager vi sikkerhedskopiering af hele deres virtuelle miljø hos os. Vi foretager sikkerhedskopiering af vores egne systemer og data på samme vis, som vores kunders systemer og data.

Vi har defineret retningslinjer for på hvilken vis, vi foretager sikkerhedskopiering. Hver nat føres en fuld kopi af data fra vores centrale systemer til vores backupsystemer. Dermed er data fysisk separeret fra vores driftssystemer, og efter endt afvikling, foretages der en automatiseret verificering af, hvorvidt datamængde og indhold mellem vores driftssystem og backupsystem, stemmer overens.

En ansvarlig medarbejder sikrer herefter, at sikkerhedskopieringen er sket og foretager det fornødne, hvis jobbet er fejlet, og herefter logføre dette.

Logning og overvågning

Hændelseslogning
Vi har opsat overvågning og logning af netværkstrafik, og vores driftsafdeling følger dette. Vi foretager ikke proaktiv overvågning af logførte hændelser, men vi følger op såfremt vi mistænker, at en hændelse kan relatere til forhold afdækket i log. Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident og problem management procedurer til sikring af, at hændelser registreres, prioriteres, styres, eskaleres og, at der foretages de nødvendige handlinger. Forløbet dokumenteres i vores hotline-system.

Beskyttelse af logoplysninger
Logs bliver uploadet til vores egen logserver.

Administrator- og operatørlog
Administrator logs sker samtidig med den normale log.

Tidssynkronisering
Vi benytter os af NTP servere fra internettet, som alle servere synkroniseres op imod.

Styring af software på driftssystemer

Via vores patch proces sikrer vi, at kun godkendt og testet opdateringer bliver installeret. Jf. vort medlemskab i BFIH sikrer vi at kritiske patches der har effekt på sikkerheden aldrig bliver installeret senere end 2 måneder fra udgivelsesdato. Drejer det sig om større ændringer bliver dette drøftet på interne driftsmøder i driftsafdelingen.

Ligeledes er vores medarbejdere bekendt med politikken vedrørende download af software.

Styring af tekniske sårbarheder
Sikkerhedsvarsler fra DK-CERT bliver monitoreret og analyseret og findes disse relevante installeres disse på vores interne systemer indenfor 1 måned fra udgivelse. Der fortages derudover løbende risikovurdering af vores interne løsninger.

Kommunikationssikkerhed

Netværksforanstaltninger
It-sikkerheden omkring systemers og datas ydre rammer, er netværket mod internettet, remote eller lignende. Sikring af data og systemer inde i netværket, og det ydre værn mod uvedkommende adgang, er af højeste prioritet hos os. Alt kabelføring internt og til/fra vores systemer er redundant hele vejen.

Sikring af netværkstjenester
Adgang til vores systemer fra vores kunder, sker enten via de offentlige netværk, hvor adgang sker via krypteret VPN-adgang, IP-whitelistning eller MPLS/VPLS. Adgang og kommunikation mellem vores servere og vores co-location, sker i et lukket netværk.

Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall.

Vi er ansvarlige for driften og sikkerheden hos os, dvs. fra og med systemerne hos os og ud til internettet (eller MPLS/VPLS). Vores kunder er selv ansvarlige for at kunne tilgå internettet.

Opdeling af netværk
Vores netværk er opdelt i flere segmenter og derved sikres det at vores interne netværk er adskilt fra kundernes netværk. Derudover er de tjenester der har følsomt data, placeret i specielt sikrede miljøer.

Politikker og procedurer for dataoverførsel
Ekstern datakommunikation sker alene via mails, idet vores kunders adgang og brug af vores servere, ikke betragtes som ekstern datakommunikation.

Førstegangskodeord til kundesystemer fremsendes via mails, men disse skal ændres ved første logon. Glemte kodeord, personoplysninger, bestillinger mv. håndteres aldrig via telefon, udelukkende på skrift og først efter vores medarbejdere har konstateret, at det er en rigtig og autoriseret person, vi har kontakt til.

Fortrolighedsaftaler
Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.

Anskaffelse, udvikling og vedligeholdelse

Sikkerhedskrav til informationssystemer

Analyse og specifikation af sikkerhedskrav
Indføres et nyt system bliver der gennemgået en række analyser og research således at dette overholder best-practice for hardning.

Procedurer for styring af ændringer
Vi har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder og tilrettelagt hensigtsmæssigt i forhold til interne forhold. Ændringer sker alene baseret på en kvalificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer. Herudover følges en proces omkring udvikling og test, og accept fra både os og fra kundens side.

Er der tale om fundamentale ændringer af de underliggende systemer der driver vores miljø, sikres det altid, som minimum, at;

- Alle ændringer drøftes, prioriteres og godkendes af ledelsen
- Alle ændringer testes
- Alle ændringer godkendes før idriftsættelse
- Alle ændringer idriftsættes på et fastsat tidspunkt efter aftale med forretningen og evt. kunder
- Der fortages fallback-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis den ikke fungerer.
- Systemdokumentationen opdateres med den nye ændring, såfremt det vurderes nødvendigt

Er der tale om en "standard change" – altså en ændring som kan godkendes uden testforløb eller risikovurdering skal kundens accept altid foreligge på skrift inden ændringen udføres.

Vores miljø er adskilt logisk og opdelt i test og produktion, hvorved vi sikre at have testet et produkt før det kommer i produktion. Via adgangskontroller sikrer, vi at kun autoriseret personale har adgang til dette.

Begrænsning af ændringer af softwarepakker
Servicepacks og system-specifikke opdateringer, der kan medføre ændringer i funktionalitet vurderes og installeres separat. Sikkerhedsopdateringer udrulles på så vidt muligt alle systemer.

Leverandørforhold

Styring af serviceydelser fra tredjepart

Styring af ændringer af serviceydelser
Når der sker ændringer internt i organisationen, herunder politikker og procedurer, samt ændringer til vores ydelser eller ydelser fra vores eksterne samarbejdspartnere, foretages der altid en risikovurdering for at afdække om ændringerne får indflydelse på vores aftale med kunderne.

Overvågning af ydelser fra tredjepart
Via opsat overvågning fra 3. Part sikrer vi at alle ydelser som bliver leveret af tredjepart overholder de krav og vilkår vi har til/med tredjepart. Vi aflægger jævnligt besøg hos tredjepart og sikrer derved at de aftalt forhold fortsat overholdes.

Styring af sikkerhedshændelser

Styring af informationssikkerhedsbrud og forbedringer

Ansvar og procedurer
Vores medarbejdere er forpligtiget til at holde sig opdaterede ved hjælp af producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.

Der er formelt udpegede systemansvarlige, og krav til de systemansvarlige er klart og formelt defineret. Det er den systemansvarliges ansvar at udarbejde og vedligeholde procedurer, som sikrer rettidig og korrekt indgriben i forbindelse med sikkerhedsbrud.

Rapportering af informationssikkerhedshændelser
Vores hotline-system, hvori vi håndterer alle sager for kunder og interne forhold, er samtidig vores system til håndtering af sikkerhedshændelser. Heri kan vi eskalere forhold således, at opgaver får højere prioritet end andre. Herudover vil sikkerhedshændelser afstedkommet fra hhv. egne observationer, alarmering ud fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, blive eskaleret fra vores hotline til driftsafdelingen med samtidig orientering til ledelsen.

Vi har etableret kontakt til hotline hos DK-CERT, hvor vi gensidigt har aftale om orientering ved væsentlige sikkerhedsrelaterede forhold vedrørende internettrafik.

Rapportering af sikkerhedssvagheder
Vores medarbejdere og eksterne samarbejdspartnere er, via de indgåede kontrakter og aftaler, forpligtet til at anmeldelse enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelsen og nødvendige tiltag kan udføres jf. de etablerede procedurer.

Beredskabsstyring

Informationssikkerhedsaspekter ved beredskabsstyring

Beredskabsplanlægning
Skulle der opstå en nødsituation, har any.cloud udarbejdet en beredskabsplan. Beredskabsplanen er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen.

Planen og procedurerne er forankret i vores driftsdokumentation og – procedurer.

Via vores medlemskab af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark), er vi forpligtet til, at vi inden for 3 dage kan retablere enhver enhed i vores datacenter. Dette sikrer vi ved, at vi har afvejet risici, klassificeret enheder i vores driftsapparat, og har procedurer der sikrer, at vi i vores beredskabsplanlægning kan foretage udskiftning af vores driftsplatform, så de leverede ydelser vil blive retableret rettidigt.

Prøvning, vedligeholdelse og revurdering af beredskabsplaner
Planen testes 1-2 gange årligt som en del af vores beredskab, så vi sikrer, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation.

Overensstemmelse

Review af informationssikkerheden

Uafhængig evaluering af informationssikkerhed
Der foretages evaluering af en ekstern it-revisor samt i forbindelse med udarbejdelse af de årlige ISAE 3402 erklæringer.

Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder
Vores medarbejdere læser it-sikkerhedspolitikken minimum en gang om året og underskriver, at de forstår og efterkommer denne. Vi har løbende kontroller, fortaget af vores ledelse, for at sikre at vores medarbejdere overholder de sikkerhedsforanstaltninger som er specificeret i vores it-sikkerhedspolitik, dette gøre sig gældende på både de fysiske og logiske forhold.

Kontrol af teknisk overensstemmelse
Vi har procedurer der sikrer opdatering af alle systemer, og implementeret omfattende overvågning af alle systemer, herunder vores kunders services. Ydermere har vi hos en anden ISO certificeret hostingudbyder et eksternt system som overvåger tilgængelighed på alle vores services. Vi har ligeledes kontroller, der sikrer, at overvågning og sikkerhed overholdes.

Ændringer i perioden

Gennem perioden fra 1/12-2016 – 30/11-2017 der sket ganske få væsentlige ændringer. Vi har øget kompetencen af vores tekniske personale i form af nyansættelser, og herudover har vi:

- Forbedret vores system til dokumentation af arbejdsopgaver
- Implementeret og dokumenteret nye produkter
- Udviklet og forbedret interne systemer

Komplementerende kontroller

any.clouds kunder er, med mindre andet er aftalt, ansvarlige for at etablere forbindelse til any.clouds servere. Herudover er any.clouds kunder, med mindre andet er aftalt, ansvarlige for:

- At det aftalte niveau for backup dækker kundens behov
- Periodisk gennemgang af kundens egne brugere
- At overholde any.clouds til hver en tid gældende Service Level Agreement som forefindes på any.clouds hjemmeside
- At der opretholdes sporbarhed i tredjeparts software, som kunden selv administrerer.

Afsnit 3: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet

Til ledelsen hos any.cloud A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om any.cloud A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af any.cloud A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hosting-ydelse i perioden 01-12-2016 til 30-11-2017, samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

any.cloud A/S' beskrivelse (afsnit 2) indeholder en række forhold, som virksomheden skal leve op til jf. virksomhedens medlemskab af BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark). Vores revision har omfattet disse forhold, og består udover de fysiske forhold, herunder server hardware, LAN, WAN og firewalls, af:

- Hvorvidt any.cloud A/S implementerer kritiske sikkerhedsopdateringer inden for 2 måneder fra frigivelse
- Hvorvidt any.cloud A/S kan retablere enheder i datacenter inden for 3 dage
- Hvorvidt any.cloud A/S lever op til BFIH's krav for "mindstemål for god hosting".

Vores konklusion udtrykkes med høj grad af sikkerhed.

any.cloud A/S' ansvar

any.cloud A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 2) og tilhørende udtalelse (afsnit 1), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret. any.cloud A/S er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål og for udformningen, implementeringen og effektiviteten af fungerende kontroller for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

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

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

REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om any.cloud A/S' beskrivelse (afsnit 2) og om udformningen og funktionaliteten 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. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle

væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformede og fungerer effektivt.

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

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

any.cloud A/S' beskrivelse i afsnit 2 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtige efter sine særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække 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. Kriterierne, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i any.cloud A/S' beskrivelse i afsnit 2 og det er på den baggrund vores vurdering,

(a) at beskrivelsen af kontroller, således som de var udformede og implementerede i hele perioden 01-12-2016 til 30-11-2017, i alle væsentlige henseender er retvisende
(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformede i hele perioden fra 01-12-2016 til 30-11-2017
(c) at kontrollerne for de særlige krav, som er foranlediget af virksomhedens medlemskab af BFIH jf. beskrivelsen i kapitel 2, var hensigtsmæssigt udformede i hele perioden fra 01-12-2016 til 30-11-2017
(d) at de testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden 01-12-2016 til 30-11-2017.

Beskrivelse af test af kontroller

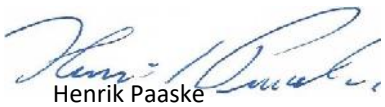
De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i det efterfølgende hovedafsnit (afsnit 4).

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt any.cloud A/S' hosting-ydelse, og deres revisorer, som har en tilstrækkelig kompetence til at vurdere den medfølgende beskrivelse sammen med anden information, herunder information om kunders egne kontroller. Denne information tjener til opnåelse af en forståelse af kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

København, 19. december 2017

REVI-IT A/S
Statsautoriseret revisionsaktieselskab



Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, CIPP/E, CRISC, adm. direktør

Afsnit 4: Kontrolmål, udførte kontroller, test og resultater heraf

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som any.cloud A/S har implementeret. Vores test af funktionaliteten har omfattet de kontroller, som vi har vurderet nødvendige for at kunne opnå en høj grad af sikkerhed for, at de anførte kontrolmål har været opnået i perioden 01-12-2016 til 30-11-2017.

Vi har således ikke nødvendigvis testet alle de kontroller, som any.cloud A/S har nævnt i sin beskrivelse i afsnit 2.

Kontroller, udført hos any.cloud A/S' kunder, er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

Vi har udført vores tests af kontroller hos any.cloud A/S via følgende handlinger:

Metode	Overordnet beskrivelse
Forespørgsel	Interview, altså forespørgsel af udvalgt personale hos virksomheden angående kontroller
Observation	Observation af, hvordan kontroller udføres
Inspektion	Gennemgang og stillingtagen til politikker, procedurer og dokumentation vedrørende kontrollers udførelse
Genudførelse af kontrol	Vi har selv udført – eller har observeret – en genudførelse af kontroller med henblik på at verificere, at kontrollen fungerer som forventet

Beskrivelse og resultat af vores tests ud fra de testede kontroller fremgår af de efterfølgende skemaer. I det omfang vi har konstateret væsentlige svagheder i kontrolmiljøet eller afvigelser herfra, har vi anført dette.

Risikovurdering og -håndtering

Risikovurdering

Kontrolmål: Formålet er at sikre, at virksomheden periodisk foretager en analyse og vurdering af it-risikobilledet.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
4.1	Risikovurdering foretages periodisk, samt når vi foretager ændringer eller implementerer nye systemer, som vi vurderer at være relevante til at revurdere vores generelle risikovurdering. Ansvaret for risikovurderinger er hos virksomhedens CTO og skal efterfølgende forankres og godkendes hos ledelsen.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af risikoanalysen indenfor perioden, og vi har inspiceret dokumentation for, at denne er gennemgået og godkendt af ledelsen i revisionsperioden.	Ingen væsentlige afvigelser konstateret.

Informationssikkerhedspolitikker

Retningslinjer for styring af informationssikkerhed

Kontrolmål: Formålet er at sikre, at der gives retningslinjer for og understøttelse af informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
5.1	Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere stabil og sikker hosting-drift til vores kunder. For at kunne gøre dette, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige. Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift. Vi opdaterer løbende it-sikkerhedspolitikken, og som minimum én gang årligt.	Vi har forespurgt til udarbejdelsen af en informationssikkerhedspolitik, og vi har inspiceret dokumentet. Vi har forespurgt til periodisk gennemgang af informationssikkerhedspolitikken, og vi har inspiceret, at dokumentet er gennemgået i revisionsperioden. Vi har desuden inspiceret kontrollen for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken, og vi har inspiceret dokumentation for ledelsesgodkendelse.	Ingen væsentlige afvigelser konstateret.

Organisering af informationssikkerhed

Intern organisering

Kontrolmål: Formålet er at sikre, at der etableres et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
6.1	Vi har en klart opdelt organisation hvad angår ansvar, og har udførlige ansvars- og rollebeskrivelser på alle niveauer lige fra ledelsesniveau til de enkelte driftsmedarbejdere. Gennem løbende dokumentation og processer sikrer vi at kunne udelukke eller minimere nøglepersonsafhængighed. Vores medarbejdere er forpligtiget til at holde sig opdaterede ved hjælp af producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder. Såfremt at vi vurderer, at et projekt ikke overholder vores informationssikkerhed, vil projektet enten blive tilrettet således, at dette efterfølgende overholder vores standard indenfor informationssikkerhed. Vurderer vi, at projektet slet ikke kan udføres eller ændres uden at stride imod vores sikkerhedspolitik, vil projektet blive kasseret.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen. Vi har desuden inspiceret kontrol for vedligeholdelsen af ansvarsbeskrivelser. Vi har forespurgt til adskillelse af adgang i forhold til funktion, og vi har inspiceret dokumentation for differentieret adgang. Vi har forespurgt til retningslinjer for kontakt med myndigheder, og vi har inspiceret retningslinjerne. Vi har forespurgt til kontakt med interessegrupper, og vi har inspiceret dokumentation for kontakt. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter, og vi har stikprøvevis inspiceret dokumentation for styring af projekter.	Ingen væsentlige afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser **Kontrolmål: Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
6.2	Vi har etableret mulighed for, at vores medarbejdere kan arbejde hjemmefra af hensyn til bl.a. driftsvagt, og vi har politik for, at udstyr (bærbare mv.) ikke benyttes til andet end arbejdsrelaterede forhold og ikke efterlades uden opsyn mv. Bærbare enheder er sikret med logon og kryptering. Vi har åbnet adgang til, at vi og vores kunder kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af mails og kalender. Ud over kode, har vi 2-factor slået til for forbedret sikkerhed. Vores medarbejdere har adgang via fjernarbejdspladser, hvor der anvendes VPN til RDS. 2-faktor beskyttelse benyttes altid, hvis der kobles op udefra.	Vi har forespurgt til styring af mobile enheder, og vi har inspiceret løsningen. Vi har forespurgt til sikring af fjernarbejdspladser, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Medarbejdersikkerhed

Før ansættelsen **Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
7.1	Vi har procedurer for ansættelse af medarbejdere og etablering af samarbejde med eksterne, hvor vi sikrer, at vi ansætter den rigtige kandidat i forhold til baggrund og kompetence. Vi har rolle- og ansvarsbeskrivelser for medarbejdere og medarbejderkategorier, så alle er bekendte med deres ansvar. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har stikprøvevis inspiceret dokumentation for processen. Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevis inspiceret indholdet af kontrakter.	Ingen væsentlige afvigelser konstateret.

Under ansættelsen

Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
7.2	I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. Vores aktiver er i høj grad vores medarbejdere, og vi fører en struktureret metodik i forhold til vores medarbejderes kvalifikationer, uddannelse og certificeringer. Der afholdes løbende, dog minimum årligt, kurser, foredrag samt andre relevante aktiviteter til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med sikkerhed og bevidstgøres om evt. nye trusler. Medarbejdere, og eksterne parter, hvor det er relevant at inkludere disse under vores sikkerhedsretningslinjer, bliver periodisk orienteret om vores sikkerhedsretningslinjer, samt når der sker ændringer. Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet.	Vi har forespurgt til ledelsens ansvar for videreformidling af politikker og procedurer, og vi har inspiceret dokumentation for tildeling af ansvar. Vi har forespurgt til videreuddannelse af personale, og vi har stikprøvevis inspiceret dokumentation for videreuddannelse. Vi har forespurgt til retningslinjer for sanktionering, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring

Kontrolmål: Formålet er at beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
7.3	Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm, samt sikre, at alle medarbejderes adgange til bygninger, systemer og data inddrages. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos virksomhedens CTO.	Vi har forespurgt til medarbejderes forpligtelse til opretholdelse af informationssikkerhed i forbindelse med ophør i ansættelse, og vi har inspiceret dokumentation for medarbejdernes forpligtelser.	Ingen væsentlige afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver

Kontrolmål: Formålet er at identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
8.1	Software, servere og netværksudstyr inkl. konfiguration er registreret til brug ved dokumentation, overblik over udstyr mv. Dokumenterne, netværkstopologier og lignende opdateres løbende ved ændringer og gennemgås minimum årligt af vores netværksspecialister. Via ansvarsfordeling og rollebeskrivelser er centrale netværksenheder, servere, periferienheder, systemer og data tilegnet systemansvarlige i vores virksomhed. Kunders data og systemer er tilegnet kundens kontaktperson. Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm., samt sikre, at alle medarbejderes adgange til bygninger, systemer og data inddrages. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos virksomhedens CTO.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevis inspiceret fortegnelser over aktiver. Vi har endvidere forespurgt til kontrol for opdatering af fortegnelser over aktiver, og vi har inspiceret kontrol for opdatering af fortegnelser over aktiver. Vi har forespurgt til oversigt af ejerskab for aktiver, og vi har inspiceret oversigten. Vi har forespurgt til retningslinjer for brugen af aktiver, og vi har inspiceret retningslinjerne. Vi har forespurgt til procedure til sikring af tilbagelevering af udleverede aktiver, og vi har inspiceret proceduren. Endvidere har vi stikprøvevis inspiceret dokumentation for tilbagelevering af aktiver.	Ingen væsentlige afvigelser konstateret.

Klassifikation af information

Kontrolmål: Formålet er at sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
8.2	*Ingen kontrolbeskrivelse angivet.*	Vi har forespurgt til politik for klassificering af information. Vi har forespurgt til mærkning af data. Vi har forespurgt til retningslinjer for håndtering af aktiver, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Mediehåndtering **Kontrolmål: Formålet er at sikre hindring af uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
8.3	Vi sikrer, i bedst muligt omfang, at vores medarbejderes bærbare medier såsom bærbar pc, mobiltelefon og lignende er konfigureret sikkerhedsmæssigt lige så højt, som resten af vores miljø, samt at det sikres, at de databærende medier opdateres, når vi foretager nye sikkerhedstiltag.	Vi har forespurgt til styring af bærbare medier. Vi har forespurgt til retningslinjer for bortskaffelse af medier. Vi har stikprøvevis inspiceret dokumentation for bortskaffelse af medier. Vi har forespurgt til transport af bærbare medier.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol

Forretningsmæssige krav til adgangsstyring **Kontrolmål: Formålet er at begrænse adgangen til information og informationsbehandlingsfaciliteter.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
9.1	Vi har politik for adgangstildeling. Politikken er en del af vores it-sikkerhedspolitik.	Vi har forespurgt til politik for styring af adgange til systemer og bygninger, og vi har inspiceret politikken. Vi har forespurgt til håndtering af adgang til netværk og netværksservices, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Administration af brugeradgange **Kontrolmål: Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
9.2	Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores kunder er dermed ansvarlige for oprettelse og nedlæggelse af brugerkonti. Alle brugere skal være personhenførbare, dvs. have tydeligt mærke med personnavn. Er der tale om servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for egentlig logon deaktiveret. Tildeling af privilegier er kontrolleret i forbindelse med vores normale brugeradministrationsproces. For vores egne brugere, gennemgår virksomhedens CTO periodisk, minimum årligt, virksomhedens interne systemer med oprettede brugere og deres adgangsniveau for at sikre mod adgang for uautoriserede personer.	Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne. Vi har stikprøvevis inspiceret dokumentation for oprettelse og nedlæggelse af brugere. Vi har forespurgt til proces for tildeling af rettigheder, og vi har inspiceret processen. Vi har forespurgt til overvågning af anvendelsen af privilegerede adgangsrettigheder, og vi har stikprøvevis inspiceret dokumentation for overvågning. Vi har forespurgt til opbevaring af fortrolige adgangskoder, og vi har inspiceret dokumentation for betryggende opbevaring. Vi har forespurgt til proces for periodisk gennemgang af brugere, og vi har inspiceret dokumentation for seneste gennemgang. Endvidere har vi forespurgt til kontrol for periodisk gennemgang af brugere, og vi har inspiceret kontrol for periodisk gennemgang.	Ingen væsentlige afvigelser konstateret.
Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
9.3	Vores it-sikkerhedspolitik beskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet. Medarbejdere skriver årligt under på, at de har læst og forstået seneste version af vores it-sikkerhedspolitik.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Styring af system- og applikationsadgang **Kontrolmål: Formålet er at forhindre uautoriseret adgang til systemer og applikationer.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
9.4	Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen. Alle medarbejdere, på tværs af både kundesystemer og egne systemer, har restriktioner omkring adgangskode. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger i forhold til udformningen af kodeordet. Koder skal skiftes regelmæssigt og være komplekse.	Vi har forespurgt til begrænsning af adgang til data, og vi har inspiceret dokumentation for begrænsning. Vi har forespurgt til procedure for sikker logon, og vi har inspiceret løsningen. Vi har forespurgt til system til styring af adgangskoder. Vi har inspiceret løsningen for styring af adgangskode-kvalitet og udvalgte konfigurationer.	Ingen væsentlige afvigelser konstateret.

Kryptografi

Kryptografiske kontroller **Kontrolmål: Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
10.1	Adgang til vores systemer fra vores kunder sker enten via de offentlige netværk, hvor adgang sker via krypteret VPN-adgang, IP-whitelisting eller MPLS/VPLS.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi. Vi har forespurgt til gennemgang af certifikater med hensyn til fornyelse, og vi har inspiceret kontrol for fornyelse af certifikater.	Ingen væsentlige afvigelser konstateret.

Fysisk sikring og miljøsikring

Sikre områder

Kontrolmål: Formålet er at forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
11.1	Vi har en aftale med den pågældende leverandør om housing af vores egne servere, og der er implementeret tilsvarende foranstaltninger mod tyveri, brand, vand og temperaturafvigelser.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør, og vi har inspiceret procedure for tildeling af adgang til driftsfaciliteter. Vi har forespurgt til overvågning af underleverandørens faciliteter, og vi har stikprøvevis inspiceret dokumentation for overvågning. Vi har inspiceret de fysiske forhold hos virksomhedens kontorer med henblik på at kontrollere den fysiske sikring. Vi har forespurgt til levering af pakker og varer.	Ingen væsentlige afvigelser konstateret.

Udstyr **Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.**			
Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
11.2	Vi modtager årligt revisorerklæring, der afdækker den fysiske sikkerhed hos vores underleverandører. Senest har vi modtaget revisorerklæringer, som dækker perioden 01/01-2016 til 31/12-2016. Erklæringen er afgivet uden forbehold. Alt databærende udstyr destrueres inden bortskaffelse for at sikre, at data ikke er tilgængeligt. Alle interne brugerkonti er centralt styret til at gå på skærmlås ved inaktivitet efter max 2 minutter. Dermed sikrer vi, at uautoriseret personale ikke opnår adgang til fortroligt data.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere understøttende forsyninger og sikring af regelmæssig vedligeholdelse af udstyret. Vi har forespurgt til sikring af kabler, og vi har inspiceret erklæring fra leverandør. Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler. Vi har observeret, at erklæring fra underleverandør dækker til og med 31-12-2016. Vi har forespurgt til periodisk eftersyn af ekstern lokation, og vi har stikprøvevis inspiceret dokumentation for eftersyn. Vi har forespurgt til politik for bortskaffelse af databærende medier, og vi har inspiceret politikken. Endvidere har vi stikprøvevis inspiceret dokumentation for sikker bortskaffelse. Vi har forespurgt til sikring af brugerudstyr uden opsyn, og vi har stikprøvevis inspiceret, at brugerudstyr låses ved inaktivitet. Vi har forespurgt til politik for ryddeligt skrivebord, og vi har inspiceret politikken.	Ingen væsentlige afvigelser konstateret.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

Kontrolmål: Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
12.1	Selvom vores organisation ikke nødvendigvis gør, at vi kan have overlap inden for alle opgaver og systemer, sikrer vi via dokumentationer og beskrivelser, at medarbejdere eller nye medarbejdere kan påbegynde et arbejde på et system, som vedkommende ikke har operationel og historisk erfaring med. • Alle ændringer drøftes, prioriteres og godkendes af ledelsen • Alle ændringer testes • Alle ændringer godkendes før idriftsættelse • Alle ændringer idriftsættes på et fastsat tidspunkt efter aftale med forretningen og kunder • Der fortages fallback-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis den ikke fungerer • Systemdokumentationen opdateres med den nye ændring, såfremt det vurderes nødvendigt. Ved standard ændringer behøver risikovurdering ikke at foreligge, ligeledes er godkendelse fra ledelsen heller ikke nødvendig. Dog kræver alle standard ændringer altid kundens accept på skrift. Vores miljø er adskilt logisk og opdelt i test og produktion, hvorved vi sikrer at have testet et produkt, før det kommer i produktion. Via adgangskontroller sikrer vi, at kun autoriseret personale har adgang til dette. Via vores generelle overvågningssystem har vi sat grænseværdier for, hvornår vores overordnede systemer, og dermed vores kunders systemer, skal skaleres op af hensyn til elektronisk plads, svartider mv.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til ændringsstyring, og vi har stikprøvevis inspiceret dokumentation for håndtering af ændringer i perioden. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Vi har forespurgt til anvendelsen af testmiljø, og vi har inspiceret dokumentation for eksistensen af testmiljø.	Ingen væsentlige afvigelser konstateret.

Malwarebeskyttelse

Kontrolmål: Formålet er at sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
12.2	Vi har implementeret scannings- og overvågningssystemer til at sikre mod kendt skadevoldende kode, dvs. hvad vi og vores kunder – via vores platforme – kan risikere at blive inficeret med på internettet, via mails mv. Vi har antivirus-systemer, anti-malware på alle platforme, systemer til overvågning af internetbrug, trafik og ressourcer på SaaS platforme, og sikringer i øvrige tekniske og centrale installationer (firewall mv.).	Vi har forespurgt til foranstaltninger mod malware. Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen.	Ingen væsentlige afvigelser konstateret.

Backup

Kontrolmål: Formålet er at beskytte mod tab af data.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
12.3	Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, og efter de aftaler, vi har med vores kunder. Vi har en test af, hvordan systemer og data praktisk kan retableres. Der føres en log over disse tests således, at vi kan følge op på, om vi kan ændre på procedurer og processer for at højne vores løsning. Med mindre andet er aftalt med vores kunder, foretager vi sikkerhedskopiering af hele deres virtuelle miljø hos os. Vi foretager sikkerhedskopiering af vores egne systemer og data på samme vis som vores kunders systemer og data. Vi har defineret retningslinjer for på hvilken vis, vi foretager sikkerhedskopiering.	Vi har forespurgt til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for opsætningen. Vi har forespurgt til opbevaring af backup, og vi har inspiceret erklæring fra underleverandør med henblik på at se, at backup opbevares forsvarligt. Vi har forespurgt til test af genopretelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse. Vi har forespurgt til periodisk genoprettelse af backupfiler, og vi har inspiceret kontrol for periodisk gennemgang for genoprettelse af backupfiler.	Ingen væsentlige afvigelser konstateret.

Logning og overvågning

Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
12.4	Vi har opsat overvågning og logning af netværkstrafik, og vores driftsafdeling følger dette. Vi foretager ikke proaktiv overvågning af logførte hændelser, men vi følger op, såfremt vi mistænker, at en hændelse kan relatere til forhold afdækket i log. Logs bliver uploadet til vores egen logserver. Administrator logs sker samtidig med den normale log. Vi benytter os af NTP servere fra internettet, som alle servere synkroniseres op imod.	Vi har forespurgt til logning af brugeraktivitet. Vi har stikprøvevis inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger, og vi har inspiceret løsningen. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.

Styring af driftssoftware

Kontrolmål: Formålet er at sikre integriteten af driftssystemer.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
12.5	Via vores patch proces sikrer vi, at kun godkendte og testede opdateringer bliver installeret. Jf. vort medlemskab i BFIH sikrer vi, at kritiske patches, der har effekt på sikkerheden, aldrig bliver installeret senere end 2 måneder fra udgivelsesdato. Ligeledes er vores medarbejdere bekendt med politikken vedrørende download af software.	Vi har forespurgt til retningslinjer for installation af software på driftssystemer, og vi har inspiceret retningslinjerne. Vi har forespurgt til rettidig opdatering af driftssystemer, og vi har inspiceret dokumentation for opdatering af driftssystemerne, som stemmer overens med BFIH's krav.	Ingen væsentlige afvigelser konstateret.

Sårbarhedsstyring

Kontrolmål: Formålet er at forhindre, at tekniske sårbarheder udnyttes.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
12.6	Sikkerhedsvarsler fra DK-CERT bliver monitoreret og analyseret, og findes disse relevante, installeres disse på vores interne systemer indenfor 1 måned fra udgivelse. Der foretages derudover løbende risikovurdering af vores interne løsninger.	Vi har forespurgt til styring af tekniske sårbarheder, og vi har inspiceret dokumentation for styringen. Vi har forespurgt til styring af adgang til programinstallation, og vi har inspiceret dokumentation for begrænsningen af brugere med rettighed til programinstallation.	Ingen væsentlige afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed

Kontrolmål: Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
13.1	Adgang til vores systemer fra vores kunder sker enten via de offentlige netværk, hvor adgang sker via krypteret VPN-adgang, IP-whitelisting eller MPLS/VPLS. Adgang og kommunikation mellem vores servere og vores co-location sker i et lukket netværk. Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall. Vores netværk er opdelt i flere segmenter, og derved sikres det, at vores interne netværk er adskilt fra kundernes netværk.	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall og patching af firewall. Vi har forespurgt til sikring af netværkstjenester, og vi har inspiceret dokumentation for betryggende sikring.	Ingen væsentlige afvigelser konstateret.

Informationsoverførsel

Kontrolmål: Formålet er at opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
13.2	Ekstern datakommunikation sker alene via mails, idet vores kunders adgang til og brug af vores servere ikke betragtes som ekstern datakommunikation. Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.	Vi har forespurgt til politikker og procedurer for dataoverførsel. Vi har forespurgt til aftaler om dataoverførsel, og vi har stikprøvevis inspiceret dokumentation af aftale om dataoverførsel. Vi har forespurgt til retningslinjer for afsendelse af fortrolig information, og vi har inspiceret retningslinjerne. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen væsentlige afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold

Kontrolmål: Formålet er at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
15.1	Via opsat overvågning fra 3. part sikrer vi, at alle ydelser som bliver leveret af tredjepart overholder de krav og vilkår, vi har til/med tredjepart. Vi aflægger jævnligt besøg hos tredjepart og sikrer derved, at de aftalte forhold fortsat overholdes.	Vi har forespurgt til formalisering af leverandøraftaler, og vi har inspiceret aftalen med henblik på at efterse hensyntagen til informationssikkerhed. Vi har inspiceret erklæring fra underleverandør med henblik på at identificere, om der er væsentlige bemærkninger, og om den er dækkende i forhold til virksomhedens aftale med leverandøren.	Ingen væsentlige afvigelser konstateret.

Styring af leverandørydelser

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

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
15.2	Via opsat overvågning fra 3. part sikrer vi, at alle ydelser som bliver leveret af tredjepart overholder de krav og vilkår, vi har til/med tredjepart. Vi aflægger jævnligt besøg hos tredjepart og sikrer derved, at de aftalte forhold fortsat overholdes.	Vi har forespurgt til overvågning af leverandørydelser, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til politik for styring af leverandørydelser, og vi har inspiceret politikken. Vi har forespurgt til kontrol for periodisk evaluering af leverandør, og vi har inspiceret kontrollen.	Ingen væsentlige afvigelser konstateret.

Styring af informationssikkerhedsbrud

Styring af informationssikkerhedsbrud og forbedringer

Kontrolmål: Formålet er at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
16.1	Der er formelt udpegede systemansvarlige, og krav til de systemansvarlige er klart og formelt defineret. Det er den systemansvarliges ansvar at udarbejde og vedligeholde procedurer, som sikrer rettidig og korrekt indgriben i forbindelse med sikkerhedsbrud. Vores medarbejdere og eksterne samarbejdspartnere er, via de indgåede kontrakter og aftaler, forpligtet til at anmeldelse enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelsen, og nødvendige tiltag kan udføres jf. de etablerede procedurer.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden inspiceret proceduren for håndtering af informationssikkerhedshændelser. Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret proceduren. Vi har forespurgt til informationssikkerhedshændelser i perioden, og vi har stikprøvevis inspiceret dokumentation for, at proceduren er fulgt.	Ingen væsentlige afvigelser konstateret.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Informationssikkerhedskontinuitet

Kontrolmål: Formålet er at sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
17.1	Beredskabsplanen er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen. Planen og procedurerne er forankret i vores driftsdokumentation og -procedurer. Planen testes 1-2 gange årligt som en del af vores beredskab, så vi sikrer, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation.	Vi har forespurgt til udarbejdelsen af en beredskabsplan til sikring af videreførelse af driften i forbindelse med nedbrud og lignende, og vi har inspiceret planen. Vi har forespurgt til implementering af kompenserende tiltag i forbindelse med test af beredskabstest, og vi har inspiceret dokumentation for implementeringen. Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test. Vi har endvidere forespurgt til revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurdering.	Ingen væsentlige afvigelser konstateret.

Redundans

Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
17.2	Vi modtager årligt revisorerklæring, der afdækker den fysiske sikkerhed hos vores underleverandører.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Overensstemmelse

Gennemgang af informationssikkerheden

Kontrolmål: Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.

Nr.	any.cloud A/S' kontrol	REVI-IT's test	Resultat af test
18.2	Vores medarbejdere læser it-sikkerhedspolitikken minimum en gang om året og underskriver, at de forstår og efterkommer denne. Vi har løbende kontroller, foretaget af vores ledelse, for at sikre, at vores medarbejdere overholder de sikkerhedsforanstaltninger, som er specificeret i vores it-sikkerhedspolitik, dette gør sig gældende for både de fysiske og logiske forhold. Vi har ligeledes kontroller, der sikrer, at overvågning og sikkerhed overholdes.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden. Vi har forespurgt til intern kontrol til sikring af overholdelse af sikkerhedspolitik og procedurer, og vi har inspiceret udvalgte kontroller. Vi har forespurgt til periodisk kontrol af teknisk overensstemmelse, og vi har inspiceret dokumentation for overvågning.	Ingen væsentlige afvigelser konstateret.