Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med hosting-ydelse i perioden 01-12-2014 til 30-11-2015

ISAE 3402-II

any.cloud A/S

CVR nr.: 31 16 15 09

december 2015

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 disses 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-aktiviteter til kunder i hele perioden fra 01-12-2014 til 30-11-2015. 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 01-12-2014 til 30-11-2015

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

(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i hele perioden fra 01-12-2014 til 30-11-2015. 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 01-12-2014 til 30-11-2015.

København, den 18. december 2015

any.cloud A/S

Gregor Møller
CEO

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

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

any.cloud A/S blev stiftet i 2007 og er et søsterselskab til it-konsulentvirksomheden any.mac A/S. any.cloud leverer professionelle ISO-certificerede cloud services til dansk erhvervsliv. Dette er any.clouds tredje ISAE3402 type II-erklæring.

any.cloud har primær hosting i det 3.500m2 store InterXion Danmark i Ballerup, som er en europæisk udbyder af cloud- og operatørneutrale datacentre med over 39 datacentre fordelt på 11 lande. any.cloud tilbyder co-lokation via lukket netværk i det 27 datacenter store, IBM-ejede, selskab Softlayer og kan herigennem levere løsninger i hele verden.

Vi tilbyder alle relevante sikkerhedsforanstaltninger som f.eks. inergen, køling, redundante strømkilder og fiberlinjer og fuldt udstyrede overvågningssystemer.

any.cloud er underlagt strenge kontrolforanstaltninger, høje sikkerhedskrav samt krav om at skabe gennemsigtighed i forhold til indhold af kvalitet og sikkerhed i IT-hosting-ydelser.

any.cloud har hovedkontor i Danmark og har yderligere afdelinger i Polen og Tjekkiet.

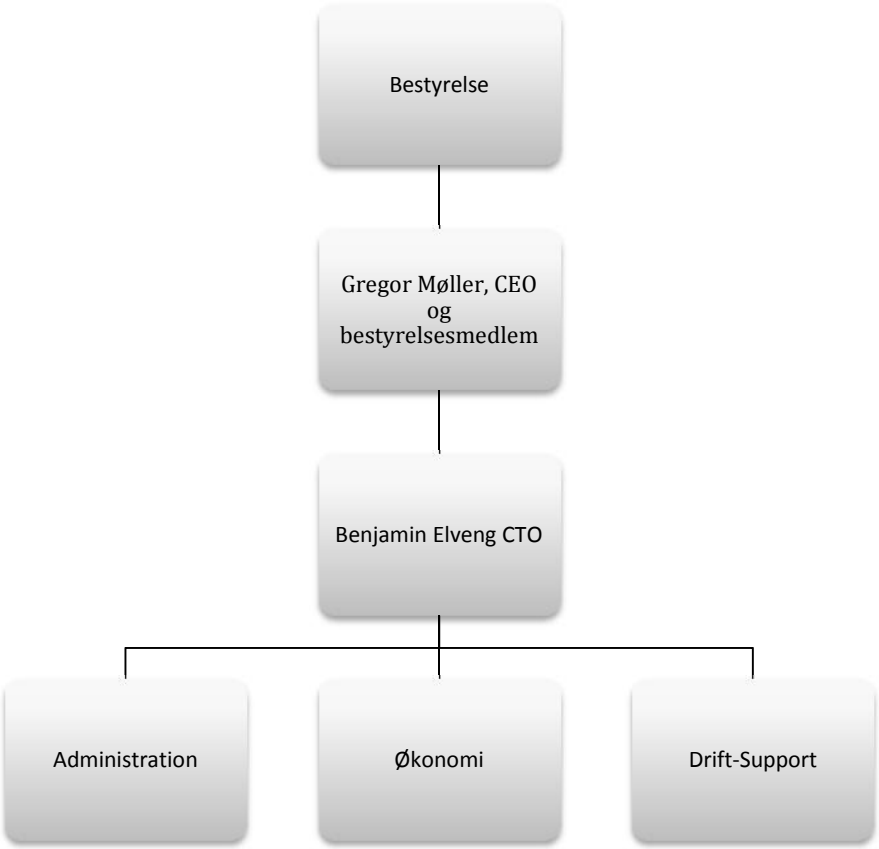
any.cloud – IT helt enkelt

any.cloud har følgende primære produkter:

- VPS (Virtual Private Server)
- Virtual hybrid-løsninger med mulighed for DRaaS (Disaster Recovery as a Service)
- Sikkerhedsprodukter
- MPLS- og fiberinfrastruktur.

Organisation og ansvar

any.cloud har en klar og gennemsigtig virksomhedsstruktur.



any.cloud beskæftiger 13 medarbejdere og er inddelt i afdelingerne Administration, Økonomi og Drift-Support. Der beskæftiges yderligere 16 medarbejdere i søsterselskabet any.mac A/S, som udfører al on-site support og drift af any.clouds kunder.

any.clouds medarbejdere arbejder således på hosting-infrastrukturen alene.

Support modtager alle indkomne forespørgsler og løser enten kundernes problemer eller videregiver opgaven til driftsafdelingen til bearbejdning.

Driftsafdelingen fungerer dermed både som 2. line support for hotline og håndterer herudover den praktiske implementering af nye kunder, overvåger bestående driftsløsninger og andet forbundet med den daglige drift af vores hostingmiljø.

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
- 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 ikke implementeret andre sikkerhedsforanstaltninger til sikring af disse enheder og disses brugeradgange.

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 Remote Desktop og IP restriction.

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 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 tydligt 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 (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 underleverandør.

Senest har vi modtaget revisorerklæringen som dækker perioden 01/01-2014 til 31/12-2014. 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.

Uanset hvilken 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.

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 procedurer for rapportering af kapacitetsproblemer.

Beskyttelse mod malware

Foranstaltninger mod malware

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, systemer til overvågning af internetbrug, trafik og ressourcer på SaaS platforme, sikringer i øvrige tekniske og centrale installationer (firewall mv.).

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 retablereres. 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. Jvf. 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.

Sikring af netværkstjenester

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.

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 følsomme 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.

Uanset hvilken 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 evt. kunder

- Der foretages 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.

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
Service packs 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 tredjepart 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.

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 evalueringen 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 hosting-udbyder 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 1/12-2014 til 30/11-2015 er 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 hostingaktiviteter i perioden 01-12-2014 til 30-11-2015, 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.

Denne erklæring er udarbejdet efter helhedsmetoden og omfatter således ledelsens beskrivelse af kontrolmål og de hertil hørende kontrolaktiviteter hos any.cloud A/S på alle områder inden for de generelle it-kontroller, som kan henføres til de leverede serviceydelser.

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 udtalelsen 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.

Vores uafhængighed og kvalitetsstyring

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

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 udformet 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 udformet og implementeret i hele perioden 01-12-2014 til 30-11-2015, 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 01-12-2014 til 30-11-2015
(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 01-12-2014 til 30-11-2015
(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 01-12-2014 til 30-11-2015.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt any.cloud A/S' hostingydelser, og disses 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, 18. december 2015

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Martin Brogaard Nielsen
It-revisor, CISA, 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 01-12-2014 til 30-11-2015.

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.

Vi har, ud fra kendskab til any.cloud A/S' organisation og standard hosting-leverance, vurderet, at område 14, Anskaffelse, udvikling og vedligeholdelse af systemer, fra ISO 27002:2013, ikke er relevant at gennemgå i forhold til virksomhedens standard hosting-leverance, idet omtalte område omhandler forhold vedr. systemudvikling.

Risikovurdering og -håndtering

Risikovurdering

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
4.1	Formålet er at sikre, at virksomheden periodisk foretager en analyse og vurdering af it-risikobilledet.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af it-risikoanalysen i perioden, og vi har verificeret, at denne er gennemgået og godkendt af ledelsen i revisionsperioden.	Ingen væsentlige afvigelser konstateret.

It-sikkerhedsstyring

It-sikkerhedspolitik

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
5.1	Formålet er at sikre, at der gives retningslinjer for og understøttelse af informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.	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 også inspiceret kontrol for periodisk gennemgang af dokumentet. Vi har forespurgt til ledelsesgodkendelse af informationssikkerhedspolitikken samt inspiceret dokumentation for ledelsesgodkendelse.	Ingen væsentlige afvigelser konstateret.

Organisering af informationssikkerhed

Intern organisering

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
6.1	Formålet er at sikre, at der etableres et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden samt inspiceret dokumentation for tildelingen og 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. Vi har forespurgt til kontakt med interessegrupper og inspiceret dokumentation for kontakt med DK-CERT. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter. Vi har stikprøvevist inspiceret projektforløb og verificeret, at der tages hensyn til informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Mobile enheder og fjernarbejdspladser

6.2	Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.	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.

Sikkerhed i forhold til HR

Inden ansættelse

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
7.1	Formålet er at sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har endvidere stikprøvevist inspiceret dokumentation for, at proceduren er fulgt. Vi har forespurgt til formaliseringen af ansættelsesforhold, og vi har stikprøvevist inspiceret indholdet af kontrakter.	Ingen væsentlige afvigelser konstateret.

Under ansættelse			
7.2	Formålet er at sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.	Vi har forespurgt til en beskrivelse af ledelsens ansvar for videreformidling af informationssikkerhedskriterier, og vi har inspiceret beskrivelsen. Vi har forespurgt til uddannelse af personalet, og vi har stikprøvevist inspiceret dokumentation for kursusdeltagelse. Vi har forespurgt til retningslinjer for sanktionering, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.
Ophør eller ændring i ansættelse			
7.3	Formålet er at sikre, at organisationens interesser, som led i ansættelsesforholdets ændring eller ophør, beskyttes.	Vi har forespurgt til formalisering af forpligtelser efter ophør af ansættelse, og vi har stikprøvevist inspiceret formaliseret aftale.	Ingen væsentlige afvigelser konstateret.

Styring af aktiver

Ansvar for aktiver			
Nr.	Kontrolmål	REVI-IT's test	Resultat af test
8.1	Formålet er at sikre, at organisationens aktiver defineres, og at der defineres passende ansvarsområder til beskyttelse heraf.	Vi har forespurgt til fortegnelser over aktiver, og vi har stikprøvevist inspiceret 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.	Det har ikke været muligt at teste effektiviteten af proceduren for tilbagelevering af aktiver, da der i perioden ikke har været fratrædelser af medarbejdere.
Mediehåndtering			
8.3	Formålet er at sikre hindring af uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.	Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for løsningen. Vi har forespurgt til retningslinjer for bortskaffelse af medier. Vi har forespurgt til transport af bærbare medier.	Ingen væsentlige afvigelser konstateret.

Adgangskontrol

Forretningskrav til adgangskontrol

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
9.1	Formålet er at sikre, at adgangen til information og informationsbehandlingsfaciliteter begrænses.	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

9.2	Formålet er at sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.	Vi har forespurgt til procedure for oprettelse og nedlæggelse af brugere, og vi har inspiceret procedurerne. Vi har stikprøvevist 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 stikprøvevist 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. Vi har forespurgt til procedure for inddragelse af rettigheder, og vi har inspiceret proceduren.	Det har ikke været muligt at teste effektiviteten af inddragelse af adgangsrettigheder for perioden, da der ikke har været ophør af medarbejdere. Dog har vi observeret, at der foreligger en procedure.

Brugeransvar

9.3	Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.	Vi har forespurgt til retningslinjer for brugen af fortrolig adgangskode, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Kontrol af adgang til systemer og data			
9.4	Formålet er at sikre, at uautoriseret adgang til systemer og applikationer forhindres.	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 og udvalgte konfigurationer.	Ingen væsentlige afvigelser konstateret.

Kryptografi

Kontrol med anvendelsen af kryptografi			
Nr.	Kontrolmål	REVI-IT's test	Resultat af test
10.1	Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevist inspiceret brugen af kryptografi.	Ingen væsentlige afvigelser konstateret.

Fysiske og miljømæssige sikringer

Sikre områder

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
11.1	Formålet er at sikre hindring af uautoriseret fysisk adgang til samt beskadigelse af og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold, og vi har inspiceret erklæringen for betryggende fysisk sikring. Vi har observeret, at erklæring fra underleverandør dækker perioden 1. januar 2014 til 31. december 2014. Vi har forespurgt til periodisk eftersyn af ekstern lokation, og vi har stikprøvevist inspiceret dokumentation for eftersyn. Vi har endvidere ved genudførelse af kontrol inspiceret den eksterne lokation. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter hos underleverandør, og vi har stikprøvevist inspiceret dokumentation for tildeling af adgang til driftsfaciliteter. Vi har inspiceret de fysiske forhold hos any.clouds kontorer med henblik på at kontrollere den fysiske sikring. Vi har forespurgt til levering af pakker og varer.	Ingen væsentlige afvigelser konstateret.

Udstyr			
11.2	Formålet er at undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold. Vi har inspiceret erklæring med det formål at identificere bemærkninger i forhold til den fysiske sikkerhed, herunder bl.a. efterset, at der er understøttende forsyninger, samt at disse serviceres. Vi har observeret, at erklæring fra underleverandør dækker perioden 1. januar 2014 til 31. december 2014. Vi har forespurgt til periodisk eftersyn af ekstern lokation, og vi har stikprøvevist inspiceret dokumentation for eftersyn. Vi har endvidere ved genudførelse af kontrol inspiceret den eksterne lokation. Vi har forespurgt til sikring af kabler, og vi har inspiceret erklæring fra leverandør. Vi har forespurgt til politik for bortskaffelse af udstyr. Vi har forespurgt til sikring af brugerudstyr uden opsyn, og vi har stikprøvevist inspiceret, at brugerudstyr låses ved inaktivitet.	Ingen væsentlige afvigelser konstateret.

Sikkerhed i forbindelse med drift

Operationelle procedurer og ansvarsområder			
Nr.	Kontrolmål	REVI-IT's test	Resultat af test
12.1	Formålet er at sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.	Vi har forespurgt til procedurer i forbindelse med driften og har stikprøvevist inspiceret procedurerne. Vi har forespurgt til ændringsstyring og har stikprøvevist inspiceret dokumentation for håndtering af ændringer i perioden. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevist 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.

Beskyttelse mod malware			
12.2	Formålet er at sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.	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			
12.3	Formålet er at beskytte mod tab af data.	Vi har forespurgt til konfiguration af backup, og vi har stikprøvevist inspiceret dokumentation for opsætningen. Vi har forespurgt til opbevaring af backup og har inspiceret erklæring fra underleverandør med henblik på at se, at backup opbevares forsvarligt. Vi har forespurgt til test af genoprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse.	Ingen væsentlige afvigelser konstateret.
Logning og overvågning			
12.4	Formålet er at registrere hændelser og generere bevis.	Vi har forespurgt til logning af brugeraktivitet, og vi har stikprøvevist inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger og har inspiceret løsningen. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen.	Ingen væsentlige afvigelser konstateret.
Styring af software på driftssystemer			
12.5	Formålet er at sikre integriteten af driftssystemer.	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.
Styring af tekniske sårbarheder			
12.6	Formålet er at sikre, at udnyttelse af tekniske sårbarheder forhindres.	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 netværkssikkerheden

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
13.1	Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.	Vi har forespurgt til foranstaltninger til beskyttelse af netværk og netværkstjenester. Vi har inspiceret dokumentation for etablering af firewall samt patching af firewall. Vi har forespurgt til sikring af netværkstjenester og har inspiceret dokumentation for betryggende sikring. Vi har forespurgt til opdeling af netværket og har inspiceret dokumentation for opdeling.	Ingen væsentlige afvigelser konstateret.

Dataoverførsler

13.2	Formålet er at opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.	Vi har forespurgt til politikker og procedurer for dataoverførsel. Vi har forespurgt til retningslinjer for afsendelse af fortrolig information. Vi har forespurgt til etablering af fortrolighedsaftaler, og vi har inspiceret dokumentation for etablering.	Ingen væsentlige afvigelser konstateret.

Leverandørforhold

Informationssikkerhed i leverandørforhold

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
15.1	Formålet er at opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.	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 til identificering af betryggende sikkerhed.	Ingen væsentlige afvigelser konstateret.

Styring af serviceydelser fra tredjepart

15.2	Formålet er at sikre, at aftalt niveau og ændringer i levering af ydelser kontrolleres.	Vi har forespurgt til overvågning af underleverandører, og vi har inspiceret dokumentation for overvågning. Vi har forespurgt til styring af ændringer hos underleverandører.	Ingen væsentlige afvigelser konstateret.

Styring af sikkerhedshændelser

Styring af informationssikkerhedsbrud og forbedringer

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
16.1	Formålet er at sikre ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har også inspiceret procedure til håndtering af informationssikkerhedshændelser. Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne. Vi har forespurgt til informationssikkerhedshændelser i perioden. Vi har forespurgt til procedure for vurdering, reaktion og evaluering af informationssikkerhedsbrud, og vi har inspiceret proceduren.	Virksomheden har en procedure for håndtering af informationssikkerhedsbrud, dog har det ikke været muligt at teste effektiviteten af proceduren, da der ikke er indtruffet informationssikkerhedshændelser i perioden.

Informationssikkerhedsaspekter ved beredskabsstyring

Beredskab i forhold til informationssikkerheden

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
17.1	Formålet er at sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for beredskabs- og reetableringsstyring.	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 test af beredskabsplan samt implementering af kompenserende tiltag i forbindelse med test af beredskabsplan, og vi har inspiceret dokumentation for test og implementering af kompenserende tiltag.	Ingen væsentlige afvigelser konstateret.

Redundans

17.2	Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Overensstemmelse

Review af informationssikkerheden

Nr.	Kontrolmål	REVI-IT's test	Resultat af test
18.2	Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.	Vi har forespurgt til uafhængig evaluering af informationssikkerheden, og vi har inspiceret, at dette foretages. 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.	Ingen væsentlige afvigelser konstateret.