Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning i forbindelse med hosting-ydelsen pr. 24. maj 2018

ISAE 3402, type I

Complea A/S

CVR-nr. 33 15 37 16

Maj 2018

Indholdsfortegnelse

Afsnit 1: Complea A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Complea A/S' hostingydelse, 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. Complea A/S bekræfter, at:

(a) Den medfølgende beskrivelse, i afsnit 2, giver en retvisende beskrivelse af Complea A/S' hostingydelse til kunder pr. 24. maj 2018. 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 identificerede 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) 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 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 pr. 24. maj 2018. 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.

Nørresundby, 24. maj 2018

Complea A/S

Morten Hovaldt
Adm. direktør

Afsnit 2: Complea A/S' beskrivelse af hosting-ydelsen samt interne kontroller

1. Indledning

Denne beskrivelse har til formål at levere information til Compleas kunder og deres revisorer vedrørende kravene til ISAE-3402. Dette er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører.

Den følgende beskrivelse omfatter kontrolmål og kontroller hos Complea A/S. Der er ikke inkluderet individuelle kundeforhold i denne beskrivelse da den er baseret på baggrund af Compleas standardservices. De implementeret kontroller har afsæt i ISO 27002, som er international standard for styring af informationssikkerhed og danner grundlagt for strukturen i IT-sikkerhedspolitikken og dermed også denne beskrivelse.

2. Complea A/S og vores hostingydelse

Complea A/S er en moderne og innovativ virksomhed, som blev grundlagt i 2010 og beskæftiger 36 medarbejdere. Hovedkontoret er placeret i Nørresundby og har ligeledes en afdeling i Frederikshavn. Tilsvarende tilbyder Complea alle løsninger som hosted via Compleas eget hostingcenter. Det betyder, at Complea kan overtager enten hele eller enkelte dele af kunders IT-Løsning. Dermed kan Complea overvåge kunders data 24/7/365 mens kunderne kan fokusere på deres kerneforretning.

Complea betjener kunder over hele landet, ligesom der også tilbydes support til kundernes udenlandske afdelinger. Målet i Complea er at være Danmarks mest innovative leverandør og servicepartner inden for IT-løsninger, telefoni og ERP-systemer samt softwareudvikling. Ligeledes arbejdes der ud fra en grundfilosofi bestående af 4 kerneværdier, som definerer Compleas DNA: Stolthed, ansvarlighed, åbenhed og fleksibilitet.

Compleas kort- og langsigtede strategi har afsæt i den fastsatte vision og mission. Strategien forgrener sig ned gennem organisationen, hvilket sikrer at alle medarbejdere arbejder mod det samme mål.

Vision: Complea A/S skal være den markedsledende samarbejdspartner inden for værdiskabende IT- og kommunikationsløsninger baseret på menneskelige værdier… det er os, som markedet kigger på!

Mission: Complea A/S dedikerede medarbejdere rådgiver, leverer og servicerer værdiskabende IT- og kommunikationsløsninger, der indfrier private og offentlige virksomheders forventninger til teknologi og effektivisering.

Support og IT drift sørger Complea for, så kundernes medarbejdere altid kan arbejde sikkert og effektivt, hvilket sikrer at de kan fokusere på deres kerneforretning.

Complea råder over eget hostingcenter, som er opbygget efter best-practice og leverer en hostingydelse med høj fleksibilitet, som kan skræddersyes efter kunders behov og krav. Dette betyder at Complea kan levere en komplet IT-platform med tilsvarende support i eget hostingcenter. Alternativt kan Complea også levere en komplet IT-platform onsite ved kunden, hvis dette ønskes.

Complea blev i 2015 kåret af Børsen, som Regional Gazellevinder for region Nordjylland på baggrund af en vækstprocent på over 600. Efterfølgende er der ligeledes vundet Gazellepriser i 2016 og 2017.

Formålet med dette kontroltjek er at sikre, at alle procedurerne i IT-sikkerhedspolitik bliver overholdt og holdes ajour, hvis der skulle forekomme organisatoriske ændringer, som har påvirkning på IT-sikkerhedspolitikken. Hele Compleas IT-sikkerhedspolitik er opbygget efter ISO 27002-standarden.

Nedenstående kontroltjeks tager udgangspunkt i IT-sikkerhedspolitikken.

4. Risikovurdering og –håndtering

Complea har udarbejdet faste procedurer for risikovurdering af forretningen og hostingcentret. Desuden sikres at alle risici er minimeret til et acceptabelt niveau, således Complea vil kunne opretholde en normal drift. Der gennemføres periodiske evaluering af risikoanalysen samt en årlig gennemgang med efterfølgende godkendelse af ledelsen.

4.1 Identificering, analyse og vurdering af risici

Der foretages løbende vurdering og registrering af eksisterende og nye risici i forbindelse med gennemførsel for projekter hos nye kunder såvel som eksistensende.

5. Sikkerhedspolitik

Den udarbejdet IT-sikkerhedspolitik sikrer at alle medarbejdere er indforstået med de fastlagte krav og rammer for IT-sikkerhed i Complea samt sikrer disse overholdes. Der gennemføres minimum en årlig revidering af IT-sikkerhedspolitikken.

IT-sikkerhedspolitikken tager udgangspunkt i at Complea ønsker at være en stærk samarbejdspartner indenfor IT-løsninger, telefoni, økonomisystemer og softwareudvikling samt sikre levering af en stabil og sikker IT-drift.

5.1 IT udstyr

Der udføres halvårligt kontroller, som sikrer at alle udleveret databærende enheder overholder IT-sikkerhedspolitikken. Der kører ligeledes en overvågning på alle PC'ere for at sikre mod installation af uautoriseret software.

5.2 Internet, E-mail og telefoni

I forbindelse med ansættelsesstart af nye medarbejdere i Complea gennemgås IT-sikkerhedspolitikken, som står beskrevet i personalehåndbogen. Personalehåndbogen ligger altid tilgængelig for alle medarbejdere i Complea.

5.3 Data

I IT-sikkerhedspolitikken foreligger klare retningslinjer for hvordan data skal behandles. Tilsvarende udføres der halvårligt kontroller, som sikrer at dette bliver overholdt.

5.4 Videoovervågning

Der er opsat videoovervågning på alle Compleas lokationer. Der er udarbejder faste procedure for opbevaring og adgang til optagelserne. Optagelserne bliver automatisk slettet efter de forskrevet tidsperioder i IT-sikkerhedspolitikken.

6. Organisering af informationssikkerhed

Complea har en standard procedure for oprettelse at nye medarbejdere, ligesom der er udarbejdet faste kontroller til at sikre, at dette bliver overholdt samt at organisationsdiagrammet bliver løbende opdateret i forbindelse med ændringer i medarbejderstaben.

6.1 Intern organisering: Complea A/S

Gennem vidensdeling og efteruddannelse sikrer Complea at alle medarbejdere efterlever den rolle, som er tiltænkt dem samt at alle procedurer bliver overholdt i forhold til IT-sikkerhedspolitikken. Dette sikrer, at sikkerhedsrelaterede forhold bliver eskaleret og håndteres jf. IT-sikkerhedspolitikken. Dette er nødvendigt,

da det er Compleas vigtigste opgave at beskytte kunders data og organisations udstyr, hvilket dermed også beskytter forretningen.

Strategien bliver årligt evalueret ligesom den fremtidig strategi bliver defineret således Complea fortsætter med at udvikle forretningen og styrke markedspositionen.

6.2 Rollefordeling

Det sikres, at alle medarbejdere besidder kompetencer indenfor deres arbejdsområde. Medarbejdernes rolle og ansvarsområde er beskrevet i deres ansættelseskontrakt samt i IT-sikkerhedspolitikken. Hvis der forekommer ændringer til dette, så er der udarbejdet en fast procedure til håndtering af ændringerne.

6.3 - Mobilt udstyr og fjernarbejdspladser

I IT-sikkerhedspolitikken er der udarbejdet et reglement for brug af mobilt udstyr og fjernarbejdspladser, som alle medarbejdere skal overholde. Dette reglement bliver gennemgået for alle nye medarbejdere i forbindelse med ansættelse hos Complea.

Der er opsat overvågning af hele Compleas netværk, hvor der kommer alarmer i forbindelse med uhensigtsmæssig adfærd. IT-sikkerhedspolitikken foreskriver ligeledes at medarbejders kodeord er personlige og det er kun medarbejderen, som må kende kodeordet. Desuden er der opsat sikring således kun autoriserede medarbejdere har adgang til systemerne. Dette sikres blandt andet via krav til password og pauseskærm i IT-sikkerhedspolitikken.

7. Medarbejdersikkerhed

Der er udarbejdet en fast procedure for medarbejdersikkerhed før, under, og efter ansættelse i Complea.

7.1 Før ansættelse

Der er en fast procedure for behandling er ansøgningerne, som sikrer at alt udleveret dokumentation fra ansøger bliver behandlet i henhold til lovningen.

7.2 Under ansættelsen

Al medarbejder data bliver opbevaret under hele ansættelsesperioden på et netværksdrev, som har opsat begrænset adgang. Der forligger en fast procedure for at sikre alle medarbejder oplysninger bliver indsamlet og opbevaret korrekt.

Der rekvireres årligt en straffeattest på alle medarbejder i Complea.

7.3 Ansættelsesforholdets ophør eller ændring

Ved ansættelsesophør bliver al medarbejder data slettet på Compleas netværk med undtagelse af skema for kontroltjek, der benyttes til at sikre at alle aktiver er tilbageleveret og alle adgange bliver deaktiveret og slettet.

8. Styring af aktiver

Al udleveret udstyr bliver dokumenteret, så der er styr på, hvad udstyr den enkelte medarbejder har fået udleveret. Der er ligeledes opsat overvågning på al udleveret udstyr, hvilket skal sikre at IT-sikkerhedspolitikken bliver overholdt.

Der er en fast procedure i forbindelse med udlevering af koder og nøgler til Compleas bygninger.

8.1 Samhandelsaftaler til kunder

Complea har automatisk overvågning af servere, storage, netværk osv. Kunder har altid mulighed for at få support 24/7/365.

Der gennemføres løbende test af backup, hvilket sikrer validering af det data, som Complea har backup af. Der forligger en fast procedure for opdatering og sikkerhedsopdatering af kunders servere.

8.2 Klassificering af data

Al data bliver betragtet som værende fortrolig og medarbejdere har adgang til data gennem de tildelte rettigheder. Der udføres stikprøver for at sikre at data bliver behandlet i henhold til IT-sikkerhedspolitikken ligesom der løbende er en revurdering af medarbejdere adgange.

8.3 Ny kunde i hostingcentret

Complea har oprettet en fast procedure for tilknytningen af kunder i hostingcentret. Desuden er der også en fast procedure for opsætning af overvågning og backup. Dette sikrer en standardiseret opsætning, hvor der er en klar fremgangsmåde i forbindelse med oprettelse af nye kunder i hosting.

8.4 Data adgang

Alle kundehenvendelser bliver registeret i Complea ticketsystem, hvor det er muligt at følge korrespondancen mellem den tildelte tekniker og kunden. Det giver også mulighed for at kontrollere og tjekket sagsforløbet efterfølgende.

Der er udarbejdet en fast procedure, hvis der skal foretages ændringer i hostingcentret. Alle ændringer bliver dokumentet af de autoriseret medarbejder i Complea og godkendt af den tekniske direktør.

8.5 Styring af flytbare medier

Da Complea har det overordnet ansvar for flytningen af data, så sikrer Complea at der ikke kan forekomme utilsigtet datalæk i forbindelse med flytning af data.

8.6 Destruktion af databærende enheder

Der ligger en fast procedure for destruktion af alle databærende medier, hvilket sikrer at det bliver gjort korrekt samt at det nødvendige dokumentation bliver lavet i forbindelse med destruktionen af mediet.

9. Adgangsstyring

Adgangsstyring bliver håndteret via Compleas domæne, som sikrer at alle medarbejdere overholder IT-sikkerhedspolitikken i forhold til adgangskode til domænet. Derudover er der logs på hvilke medarbejdere der er logget på via fjernadgang.

9.1 Forretningsmæssige krav til adgangsstyring

Der er en fast procedure for adgangsstyring jf. IT-sikkerhedspolitikken. Denne procedure bliver revurderet løbende samt i forbindelse med ændringer i medarbejderstaben.

9.2 Efteruddannelse og vidensdeling

Medarbejderne i Complea betragtes som det vigtigste aktiv og derfor er det vigtigt løbende at sikre medarbejdernes kompetencer, uddannelse og certificering. Der afholdes derfor løbende interne foredrag for at sikre at alle medarbejdere holdes ajour med Compleas sikkerhedskrav ligesom medarbejder kommer på efteruddannelse under ansættelsesperioden.

Der er en fast procedure, som sikrer disse foredrag bliver afholdt og dokumenteret.

9.3 Administration af brugeradgang

Størstedelen af alle kunders henvendelser bliver registeret i Compleas ticketsystem, hvori kunders kontaktpersoner er oprettet, så medarbejderne altid kan sikre om opgaven skal godkendes hos kundens kontaktperson inden opgaven udføres.

9.4 Adgang til IT-systemerne

Der er en fast procedure for tildeling af adgange for de enkelte medarbejdere. Der foretages løbende revideringer af tildelt adgang ligesom der er et begrænset antal medarbejdere, som kan tildele adgange.

9.5 Adgangsoversigt

Sikkerhed er et nøgleord for Complea og derfor er der lavet en adgangsoversigt, som giver et overblik over hvilket adgang den enkelte medarbejder har. Der gennemføres løbende revidering af disse adgange ligesom der foretages en gennemgang i forbindelse med ændringer i medarbejderstaben.

11. Fysisk sikring og miljøsikring

Complea har en adgangsoversigt, som viser hvilke lokationer de enkelte medarbejdere har adgang til. Denne oversigt bliver revurderet løbende ligesom den gennemgås i forbindelse med ændringer i medarbejderstaben.

Der er installeret tyverialarm på alle Compleas lokationer ligesom der er opsat videoovervågning både indendørs og udendørs. Der bliver foretaget en log i forbindelse med deaktivering af tyverialarmen, hvilket gør sig også gældende på alle lokationer.

Hovedkontoret er indhegnet og det er ikke muligt at tilgå bygningen uden at blive mødt af Complea personale i receptionen.

11.3 Hostingcentret

Compleas eget hostingcenter, som er opført i 2017, er ligeledes indhegnet og kun autoriseret personale har adgang til bygningen. Denne adgang bliver gennemgået årligt. Der er også installeret videoovervågning og tyverialarm.

Hoveddøren er altid låst og kan kun åbnes af medarbejder med adgangskort. Eksterne personer (leverandører eller kunder) kan kun få adgang til hostingcentret i følgeskab med en autoriseret medarbejder.

Der er opsat overvågning i hostingcentret med hensyn til strømafbrydelser, temperatur, brand, vand og luftfugtighed.

Hostingcentret har en høj grad af redundans og er opført på baggrund af best-practices. Der foretages jævnlige test af diesel generator. Tilsvarende udføres der et årligt kontroltjek af leverandøren på diesel generatoren. Ydermere gennemføres der test af vandkølingsanlægget, luftfilteret, ventilationen, lænse pumpe og brandslukker. Der foreligger en fast procedure for disse test.

12. Driftssikkerhed

Der køre dagligt en scanning på medarbejder PC'ere, som er logget på Compleas domæne, der sikre at ikke uautoriseret programmer er installeret, ligesom der foretages løbende stikprøver for at sikre, at dette bliver overholdt.

12.1 Driftsprocedurer og ansvarsområder

Der forligger en fast procedure for ændringer i hostingcentret. Alle ændringer er dokumentet og godkendt af den tekniske direktør. Derudover er der overvågning på alt essentielt udstyr i hosting og sender en alarm hvis der skulle forekomme uønskede hændelser.

12.2 Malwarebeskyttelse

TrendMicro, som benyttes til malwarebeskyttelse, vil altid været installeret på medarbejdere PC'er, da der er oprettet et GPO som sikre at programmet bliver installeret hvis det er blevet afinstalleret. Derudover er der opsat alarmer hvis der forekommet trusler, manglende licenser og uregelmæssig adfærd.

12.3 Patching af systemer

Complea sikrer via en fast procedure at alle relevante opdateringer, som patches, fixes og service packs bliver installeret. Det sikrer at patching af systemer bliver implementeret og kontrolleret således systemerne sikres mod nedetid og uautoriseret adgang.

Complea har en fall back plan i forbindelse med udførsel af patch management.

12.4 Backup

Der er overvågning på alle backup jobs, som bliver udført i forskellige tidsintervaller. Hvis der skulle forekomme uhensigtsmæssige hændelser, så bliver alert teamet informeret, således der kan tages action og den utilsigtede hændelse kan udbedres.

12.5 Logning

Alle logs er personhenførbar således Complea sikrer, at der altid kan spores hvilken medarbejder, som har været på hvilken server. Der foretages løbende en kontrol af hændelseslogning.

13. Kommunikationssikkerhed

Der er udarbejdet en fast procedure for oprettelse af kunder i hosting. Disse bliver gennemgået årligt for at sikre at de er aktuelle og up-to-date.

13.1 Styring af netværkssikkerhed

Complea installerer en firewall på alle installationer og åbner kun de nødvendige adgange, således kun godkendt netværkstrafik kan komme gennem firewallen. IT-sikkerhedspolitikken foreskriver hvordan medarbejdere tilgå kunders servere og systemer.

13.2 Informationsoverførsel

Alle kunde henvendelser bliver registeret i Compleas ticketsystem. Complea overfører aldrig data til 3. partsvirksomheder uden godkendelse fra kunden. Dette skal godkendes skriftligt fra kunden.

IT-sikkerhedspolitikken gennemgås i forbindelse med opstart i Complea, sådan nye medarbejder er indforstået med sikkerhedspolitikken.

14. Anskaffelse, udvikling og vedligeholdelse af systemer

Der foreligger en fast procedure for anskaffelse af nyt system, som sikre at systemet lever op til kravspecifikationen og det er ordentlig gennemtestet inden implementering. Desuden opdateres risikoanalysen, hvis dette er nødvendigt i forbindelse med indkøbet af nyt system.

15. Leverandørforhold

Der er indgået en aftale med alle leverandør, som bliver revideret hvis der forekommer større ændringer hos enten leverandøren eller Complea.

15.1 Styring af leverandørydelser

Der rekvireres årligt en revisor erklæring fra alle Compleas leverandører, som leverer en driftskritisk ydelse for Complea.

16. Styring af informationssikkerhedsbrud

Den tekniske direktør er systemansvarlig på alle Compleas systemer og informerer ud i organisationen, hvis der skulle forekomme ændringer i de systemer, som Complea benytter og tilbyder.

Ticketsystemet benyttes til håndtering af størstedelen af alle kunde henvendelser. I ticketsystemet er det muligt at eskalere forhold, således opgaver får en højere prioritering end andre.

Medarbejder og eksterne samarbejdspartnere er forpligtet til at anmelde sikkerhedshændelse til nærmeste leder jf. de indgået kontrakter, aftaler samt IT-sikkerhedspolitikken. Dette skal sikre, at der kan reageres hurtigst muligt på evt. hændelser.

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Der er udarbejdet en beredskabsplan i tilfælde af sikkerhedsbrud. Alle involveret parter er informeret om deres rolle, hvis der skulle forekomme en hændelse, som kræver af beredskabsplanen aktiveres. Beredskabsplan godkendes af ledelsen og testes årligt.

Beredskabsplanen er udleveret til de medarbejdere, som indgår i beredskabet, sådan de involverede medarbejdere altid har beredskabsplanen til rådighed.

17.1 Redundans

Der er overvågning og lavet redundans på alt drift kritisk udstyr i hostingcentret.

18. Overensstemmelse

Complea foretager løbende en vurdering om nye projekter/kunder skal udføres eller afvises. Desuden er der løbende opdatering af risikoanalysen, hvis der tages projekter/kunder ind, som er underlagt særlig lovgivning, der kan have indflydelse på forretningen.

18.1 Gennemgang af informationssikkerhed

Der foretages årligt en evaluering af alle Compleas procedurer af en ekstern IT-revisor i forbindelse med den årlige ISAE-3402 erklæring.

Komplementerende kontroller

Compleas kunder er, med mindre andet er aftalt, ansvarlige for:

- At periodisk gennemgang af kundens egne brugere.
- At der opretholdes sporbarhed i tredjeparts software som kunden selv administrerer.
- At udstyr, som ikke er leveret af Complea, bliver opdateret.
- Internet, som ikke er leveret af Complea, er funktionelt.

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

Til ledelsen hos Complea A/S, Complea A/S' kunder og deres revisorer.

Omfang

Vi har fået til opgave at afgive erklæring om Complea A/S' beskrivelse, som er gengivet i afsnit 2. Beskrivelsen, som i afsnit 1 er bekræftet af Complea A/S' ledelse, dækker virksomhedens behandling af kunders transaktioner på virksomhedens hostingydelse pr. 24. maj 2018 samt udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Complea A/S' ansvar

Complea 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. Complea A/S er herudover ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmål, og for udformningen, implementeringen og effektiviteten af kontrollerne 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 Complea A/S' beskrivelse (afsnit 2) og om udformningen 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.

Opgaven med afgivelse af en erklæring med sikkerhed om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning. 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. 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.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i beskrivelsen, og udtrykker derfor ingen konklusion herom.

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

Complea 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.

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 Complea A/S' beskrivelse i afsnit 2, og det er på den baggrund vores vurdering,

(a) at beskrivelsen af hostingydelsen, således som den var udformet og implementeret pr. 24. maj 2018, 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 pr. 24. maj 2018.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt Complea A/S' hostingydelse, 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, 24. maj 2018

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

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