Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i forbindelse med hostingydelser i perioden 25-05-2018 til 30-04-2019

ISAE 3402-II

Complea A/S

CVR-nr.: 33 15 37 16

Maj 2019

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 i hele perioden fra 25-05-2018 til 30-04-2019. 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 implementerede 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) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 25-05-2018 til 30-04-2019

(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 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 25-05-2018 til 30-04-2019. 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 25-05-2018 til 30-04-2019.

Aalborg, 31. maj 2019

Complea A/S

Morten Hovaldt
Adm. direktør

Afsnit 2: Complea A/S' beskrivelse af kontroller i forbindelse med drift af deres hostingydelse

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 27007, som er international standard for styring af informationssikkerhed og danner grundlaget for strukturen i IT-sikkerhedspolitikken og dermed også denne beskrivelse.

Complea A/S og vores hostingydelse

Complea A/S er en moderne og innovativ virksomhed, som blev grundlagt i 2010 og beskæftiger 38 medarbejdere. Hovedkontoret er placeret i Nørresundby og har ligeledes et filial 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 og backup kunders data 24/7/365 mens kunderne kan fokusere på deres kerneforretning.

Complea betjener kunder over hele landet og der tilbyder ligeledes 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. Ligeledes skal kontroltjekket sikre at hvis der forekomme organisatoriske ændringer bliver de behandlet og dokumenteret i henhold til IT-sikkerhedspolitikken. Hele Compleas IT-sikkerhedspolitik er opbygget efter ISO 27002-standarden.

Nedenstående kontroltjeks tager udgangspunkt i IT-sikkerhedspolitikken.

Risikovurdering og –håndtering

Complea har udarbejdet faste procedurer for risikovurdering af forretningen og hostingcenteret. Desuden sikres det at alle risici er minimeret til et acceptabelt niveau. Dette sikre at Complea kan opretholde en normal drift i tilfælde af en risici indtræffer.

Der gennemføres periodiske evaluering af risikoanalysen samt en årlig gennemgang med efterfølgende godkendelse af ledelsen.

Identificering, analyse og vurdering af risici

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

Sikkerhedspolitik

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

IT-sikkerhedspolitikken tager udgangspunkt i at Complea ønsker at være en stærk samarbejdspartner inden for IT-løsninger, telefoni, ERP og softwareudvikling samt sikrer levering af en stabil og sikker IT-drift.

IT udstyr

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

Internet, E-mail og telefoni

I forbindelse med ansættelses af nye medarbejdere i Complea gennemgås IT-sikkerhedspolitikken, som står beskrevet i personalehåndbogen. Personalehåndbogen er altid tilgængelig for alle medarbejdere. Hvis der bliver foretaget ændringer i personalehåndbogen informeres alle medarbejdere om tilføjelsen.

Data

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

Videoovervågning

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

Organisering af informationssikkerhed

Complea har en standard procedure for oprettelse at ansættelse nye medarbejdere. Der er tilsvarende udarbejdet faste kontroller, som sikrer at proceduren bliver overholdt samt at organisationsdiagrammet bliver løbende opdateret i forbindelse med ændringer i medarbejderstaben.

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 ift. 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 sine forretning samt styrke sin markedsposition.

Rollefordeling

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

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.

Medarbejdersikkerhed

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

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.

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.

Ansættelsesforholdets ophør eller ændring

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

Styring af aktiver

Al udleveret udstyr bliver dokumenteret, så der er styr på hvad udstyr den enkelte medarbejder har fået udleveret. Der er opsat overvågning på al udleveret udstyr, således der kan udføres kontroller, som sikre at IT-sikkerhedspolitikken bliver overholdt.

Der er en fast procedure i forbindelse med udlevering af koder og adgangskort til Compleas filialer.

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 validerer at den data som Complea har backup af og kan genskabes hvis det bliver nødvendigt. Der forligger en fast procedure for opdatering og sikkerhedsopdatering af kunders servere.

I forbindelse med opstart af nye kunder udleveres en databehandleraftale jf. persondataloven. Der ligger en fast procedure for at sikre at denne aftale bliver sendt og returneret med underskrift.

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 evaluering af medarbejdere adgange.

Ny kunde i hostingcenteret

Complea har oprettet en fast procedure for tilknytningen af kunder i hostingcenteret. 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.

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 hostingcenteret. Alle ændringer bliver dokumentet af de autoriseret medarbejder i Complea og godkendt af den tekniske direktør.

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.

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.

Adgangsstyring

Adgangsstyring bliver håndteret via Compleas domæne, som sikrer at alle medarbejdere overholder IT-sikkerhedspolitikken i forhold til adgangskode til domænet. Desuden bliver der registeret hvilket medarbejdere, som logget på via fjernadgang.

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.

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.

Administration af brugeradgang

Størstedelen af alle kunders henvendelser bliver registeret i Compleas ticketsystem, hvori kunders kontaktpersoner er oprettet. Det er med til at sikre at kunde henvendelser altid bliver godkendt at kundens kontaktperson inden opgaven udføres.

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.

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.

Kryptografi

Complea anvender Kryptografi til beskyttelses af data og forbindelser ligesom Complea ligeledes står for administrationen af krypteringsnøgler.

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 filialer ligesom der er opsat videoovervågning både indendørs og udendørs. Der bliver foretaget en log i forbindelse med deaktivering af alarmen.

Der er opsat adgangskontrol på dørene i Compleas filialer og når en medarbejder benyttes sig af sit udleveret adgangskort bliver der registeret hvornår og hvilken dør medarbejder benytter. Dette gør sig også gældende hvis der benyttes en dør, hvor medarbejderen ikke har adgang.

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

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. Hostingcenteret er bygget af ikke-brændbart materiale (gulv, loft osv.). Der var i forbindelse med opførelsen en tæt dialog med brandmyndighederne for sikre at bygningen er tilstrækkelig beskyttet mod brand.

Hostingcenteret

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

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

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

Driftssikkerhed

Der kører dagligt en scanning på medarbejdere PC'erne, som er logget på Compleas domæne. Det sikrer at ikke uautoriseret programmer er installeret, ligesom der foretages løbende stikprøver for at sikre, at det bliver overholdt.

Driftsprocedurer og ansvarsområder

Der forligger en fast procedure for ændringer i hostingcenteret. 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.

Malwarebeskyttelse

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

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.

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.

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.

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.

Styring af netværkssikkerhed

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

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.

Anskaffelse, udvikling og vedligeholdelse af systemer

Der foreligger en fast procedure for anskaffelse af nyt system, som sikrer 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.

Leverandørforhold

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

Styring af leverandørydelser

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

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.

Medarbejdere 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.

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.

Redundans

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

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.

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, deres udformning, funktionalitet og effektivitet

Til ledelsen hos Complea A/S, deres 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 i perioden 25-05-2018 til 30-04-2019, samt udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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 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 Complea 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 præ-

sentation 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

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. 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 Complea 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 25-05-2018 til 30-04-2019, 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 25-05-2018 til 30-04-2019
(c) 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 25-05-2018 til 30-04-2019.

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 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, 31. maj 2019

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 Complea 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 25-05-2018 til 30-04-2019.

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

Kontroller udført hos Complea 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 Complea 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
4.1	Der foretages løbende vurdering/revurdering og registrering af eksisterende og nye risici i forbindelse med gennemførsel for projekter hos nye kunder såvel som eksisterende.	Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse. Vi har forespurgt til evaluering af it-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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
5.1	Den udarbejdet IT-sikkerhedspolitik sikrer at alle medarbejdere er indforstået med de fastlagte krav og rammer for IT-sikkerhed i Complea samt at disse overholdes. Der gennemføres minimum en årlig revidering af IT-sikkerhedspolitikken. Der udføres halvårligt kontroller, som sikrer at alle udleveret databærende enheder overholder IT-sikkerhedspolitikken. I forbindelse med ansættelses af nye medarbejdere i Complea gennemgås IT-sikkerhedspolitikken, som står beskrevet i personalehåndbogen. Personalehåndbogen er altid tilgængelig for alle medarbejdere. Hvis der bliver foretaget ændringer i personalehåndbogen informeres alle medarbejdere om tilføjelsen	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 kontrol 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
6.1	Gennem vidensdeling og efteruddannelse sikrer Complea at alle medarbejdere efterlever den rolle, som er tiltænkt dem samt at alle procedurer bliver overholdt ift. 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 sine forretning samt styrke sin markedsposition.	Vi har forespurgt til tildeling af ansvar for informationssikkerheden, og vi har inspiceret dokumentation for tildelingen og vedligeholdelsen af ansvarsbeskrivelser fra det øverste punkt i "udført arbejde." 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 vi har inspiceret dokumentation for kontakt. Vi har forespurgt til hensyntagen til informationssikkerhed ved styring af projekter. Vi har inspiceret proceduren for projekthåndtering, herunder løsning til sagsstyring, og vi har verificeret, at der tages hensyn til informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Mobilt udstyr og fjernarbejdspladser

Kontrolmål: Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
6.2	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.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
7.1	Der er en fast procedure for behandling er ansøgningerne, som sikrer at alt udleveret dokumentation fra ansøger bliver behandlet i henhold til lovningen.	Vi har forespurgt til procedure for ansættelse af nye medarbejdere, og vi har inspiceret proceduren. Vi har endvidere stikprøvevis inspiceret dokumentation for, at proceduren er fulgt. 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
7.2	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.	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. Vi har forespurgt til retningslinjer for sanktionering.	Ingen væsentlige afvigelser konstateret.

Ansættelsesforholdets ophør eller ændring

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

Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
7.3	Ved ansættelsesophør bliver al medarbejder data slettet på Compleas netværk med undtagelse af skema for kontroltjeks, der benyttes til at sikre at alle aktiver er tilbageleveret og alle adgange bliver deaktiveret og slettet.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
8.1	Al udleveret udstyr bliver dokumenteret, så der er styr på hvad udstyr den enkelte medarbejder har fået udleveret. Der er opsat overvågning på al udleveret udstyr, således der kan udføres kontroller, som sikre at IT-sikkerhedspolitikken bliver overholdt. Der er en fast procedure i forbindelse med udlevering af koder og adgangskort til Compleas filialer.	Vi har forespurgt til fortegnelser over aktiver, og vi har inspiceret løsningen til registrering af aktiver. Vi har forespurgt til oversigt over 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.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
8.2	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 evaluering af medarbejdere adgange.	Vi har forespurgt til politik for klassificering af data, og vi har inspiceret politikken. 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
8.3	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. 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.	Vi har forespurgt til styring af bærbare medier, og vi har inspiceret dokumentation for retningslinjer. Vi har forespurgt til retningslinjer 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
9.1	Adgangsstyring bliver håndteret via Compleas domæne, som sikrer at alle medarbejdere overholder IT-sikkerhedspolitikken i forhold til adgangskode til domænet. Desuden bliver der registeret hvilket medarbejdere, som logget på via fjernadgang. Der er en fast procedure for adgangsstyring jf. IT-sikkerhedspolitikken. Denne procedure bliver revurderet løbende samt i forbindelse med ændringer i medarbejderstaben.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
9.2	Størstedelen af alle kunders henvendelser bliver registeret i Compleas ticketsystem, hvori kunders kontaktpersoner er oprettet. Det er med til at sikre at kunde henvendelser altid bliver godkendt at kundens kontaktperson inden opgaven udføres. 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.	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. 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.	Ingen væsentlige afvigelser konstateret.

Brugernes ansvar **Kontrolmål: Formålet er at gøre brugere ansvarlige for at sikre deres autentifikationsinformation.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
9.3	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.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
9.4	Der er en fast procedure for adgangsstyring jf. IT-sikkerhedspolitikken. Denne procedure bliver revurderet løbende samt i forbindelse med ændringer i medarbejderstaben. Størstedelen af alle kunders henvendelser bliver registeret i Compleas ticketsystem, hvori kunders kontaktpersoner er oprettet. Det er med til at sikre at kunde henvendelser altid bliver godkendt at kundens kontaktperson inden opgaven udføres.	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

Kryptografiske kontroller **Kontrolmål: Formålet er at sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
10.1	Complea anvender Kryptografi til beskyttelses af data og forbindelser ligesom Complea ligeledes står for administrationen af krypteringsnøgler.	Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
11.1	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 filialer ligesom der er opsat videoovervågning både indendørs og udendørs. Der bliver foretaget en log i forbindelse med deaktivering af alarmen. Der er opsat adgangskontrol på dørene i Compleas filialer og når en medarbejder benyttes sig af sit udleveret adgangskort bliver der registeret hvornår og hvilken dør medarbejder benytter. Dette gør sig også gældende hvis der benyttes en dør, hvor medarbejderen ikke har adgang. Hovedkontoret er indhegnet og det er ikke muligt at tilgå bygningen uden at blive mødt af Complea personale i receptionen. Hostingcenteret er bygget af ikke-brændbart materiale (gulv, loft osv.). Der var i forbindelse med opførelsen en tæt dialog med brandmyndighederne for sikre at bygningen er tilstrækkelig beskyttet mod brand.	Vi har forespurgt til sikring af fysiske forhold, og vi har inspiceret disse via opsat overvågning samt relaterede systemer for betryggende fysisk sikring. Vi har forespurgt til tildeling og nedlæggelse af adgang til driftsfaciliteter, og vi har inspiceret dokumentation for system til tildeling af adgang til driftsfaciliteter. Vi har inspiceret de fysiske forhold hos virksomhedens kontorer med henblik på at kontrollere den fysiske sikring.	Vi har observeret, at der ikke er opsat automatisk brandslukning i virksomhedens datacenterlokation. Ingen væsentlige afvigelser konstateret i øvrigt.

Udstyr **Kontrolmål: Formålet er at undgå tab, skade, tyveri, eller kompromittering af aktiver og driftsafbrydelse i organisationen.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
11.2	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 hostingcenteret i følgeskab med en autoriseret medarbejder. Der er opsat overvågning i hostingcenteret med hensyn til strømafbrydelser, temperatur, brand, vand og luftfugtighed. Hostingcenteret har en høj grad af redundans og er opført på baggrund af best-practices. Der udføres jævnlige test af diesel generator. Tilsvarende udføres der et årligt kontroltjek af leverandøren på diesel generatoren ligesom der gennemføres test af vandkølingsanlægget, luftfilteret, ventilationen, lænse pumpe og brandslukker. Der foreligger en fast procedure for disse tests.	Vi har forespurgt til erklæring fra underleverandør af fysiske forhold vedrørende understøttende forsyninger, 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 politik for bortskaffelse af udstyr. Vi har forespurgt til sikring af udstyr uden for virksomhedens lokaler. Vi har observeret, at erklæring fra underleverandør dækker til og med 31-12-2018. 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. Vi har forespurgt til sikring af brugerudstyr uden opsyn, og vi har inspiceret teknisk foranstaltning for, at brugerudstyr låses ved inaktivitet. Vi har forespurgt til politik for ryddeligt skrivebord.	Ingen væsentlige afvigelser konstateret.

Driftssikkerhed

Driftsprocedurer og ansvarsområder

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

Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
12.1	Der forligger en fast procedure for ændringer i hostingcenteret. 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.	Vi har forespurgt til procedurer i forbindelse med driften, og vi har stikprøvevis inspiceret procedurerne. Vi har forespurgt til ændringsstyring, og vi har inspiceret procedurerne for ændringsstyring. Vi har desuden observeret sagsgangen for, at ændringshåndtering finder sted på hensigtsmæssig vis. Vi har forespurgt til overvågning af kapacitet, og vi har stikprøvevis inspiceret dokumentation for overvågning af kapacitet. Vi har forespurgt til anvendelsen af testmiljø.	Ingen væsentlige afvigelser konstateret.

Malwarebeskyttelse

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

Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
12.2	Der kører dagligt en scanning på medarbejdere PC'erne, som er logget på Compleas domæne. Det sikrer at ikke uautoriseret programmer er installeret, ligesom der foretages løbende stikprøver for at sikre, at det bliver overholdt. TrendMicro, som benyttes til malwarebeskyttelse, vil altid været installeret på medarbejdere PC'er, da der er oprettet et GPO som sikrer at programmet altid er installeret, også hvis det er blevet afinstalleret. Derudover er der opsat alarmer hvis der forekommet trusler, manglende licenser eller uregelmæssig adfærd.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
12.3	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.	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 genopprettelse fra backupfiler, og vi har inspiceret dokumentation for test af genoprettelse.	Ingen væsentlige afvigelser konstateret.
Logning og overvågning **Kontrolmål: Formålet er at registrere hændelser og tilvejebringe bevis.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
12.4	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.	Vi har forespurgt til logning af brugeraktivitet, og vi har inspiceret logningskonfigurationerne. Vi har forespurgt til sikring af logoplysninger, og vi har inspiceret retningslinjerne. Vi har forespurgt til synkronisering op imod en betryggende tidsserver, og vi har inspiceret konfigurationerne.	Ingen væsentlige afvigelser konstateret.

Styring af driftssoftware **Kontrolmål: Formålet er at sikre integriteten af driftssystemer.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
12.5	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.	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.	Ingen væsentlige afvigelser konstateret.
Sårbarhedsstyring **Kontrolmål: Formålet er at forhindre, at tekniske sårbarheder udnyttes.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
12.6	Virksomhedens kontrolbeskrivelser behandler ikke området.	Vi har forespurgt til styring af tekniske sårbarheder, og vi har inspiceret løsningen til identificering af sårbarheder. Vi har forespurgt til fremgangsmåde for begrænsninger af softwareinstallationer, og vi har inspiceret retningslinjerne.	Ingen væsentlige afvigelser konstateret.

Kommunikationssikkerhed

Styring af netværkssikkerhed **Kontrolmål: Formålet er at sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
13.1	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. Complea installerer en firewall på alle installationer og åbner kun for de nødvendige adgange, således kun godkendt netværkstrafik kan komme gennem firewallen. IT-sikkerhedspolitikken foreskriver hvordan medarbejdere tilgå kunders servere og systemer.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
13.2	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.	Vi har forespurgt til politikker og procedurer for dataoverførsel. Vi har forespurgt til aftaler om 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 **Kontrolmål: Formålet er at sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
15.1	Der er indgået en aftale med alle leverandør, som bliver revideret hvis der forekommer større ændringer hos enten leverandøren eller Complea. Der rekvireres årligt en revisor erklæring fra alle Compleas leverandører, som leverer en driftskritisk ydelse for Complea.	Vi har forespurgt til formalisering af leverandøraftaler. 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
15.2	Der er indgået en aftale med alle leverandør, som bliver revideret hvis der forekommer større ændringer hos enten leverandøren eller Complea. Der rekvireres årligt en revisor erklæring fra alle Compleas leverandører, som leverer en driftskritisk ydelse for Complea.	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 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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
16.1	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. Medarbejdere 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.	Vi har forespurgt til ansvar og procedurer ved informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling. Vi har desuden 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.	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.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
17.1	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.	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 beredskabsplanen, og vi har inspiceret dokumentation for udført test.	Ingen væsentlige afvigelser konstateret.

Redundans

Kontrolmål: Formålet er at sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
17.2	Der er overvågning og lavet redundans på alt drift kritisk udstyr i hostingcenteret.	Vi har forespurgt til tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger.	Ingen væsentlige afvigelser konstateret.

Overensstemmelse

Overensstemmelse med lov- og kontraktkrav

Kontrolmål: Formålet er at forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav.

Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
18.1	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.	Vi har forespurgt til virksomhedens procedurer og politikker for at sikre overholdelse af lovgivning, licensbetingelser og øvrig regulering.	Ingen væsentlige afvigelser konstateret.

Gennemgang af informationssikkerheden **Kontrolmål: Formålet er at sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.**			
Nr.	Complea A/S' kontrol	REVI-IT's test	Resultat af test
18.2	Der foretages årligt en evaluering af alle Compleas procedurer af en ekstern IT-revisor i forbindelse med den årlige ISAE-3402 erklæring.	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 årshjulet for udførsel af periodisk kontrol.	Ingen væsentlige afvigelser konstateret.