et trygt samfund med it og data

Revisorerklæring

# Complea A/S

ISAE 3402 type 2 erklæring om generelle it-kontroller relateret til leverancen af hostingydelser for perioden 1. januar 2021 til 31. december 2021.

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, 1200 København K
CVR: 30 98 85 31 | Tlf. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

Februar 2022

Indholdsfortegnelse

# Afsnit 1: Beskrivelse af Complea A/S' ydelser i forbindelse med drift af hosting-platform samt generelle it-kontroller relateret hertil.

## Beskrivelse af ydelse fra Complea A/S i forbindelse med leverance af Hosting

I det følgende beskrives Compleas ydelser til kunder, som er omfattet af de generelle it-kontroller, som erklæringen omhandler. Erklæringen omfatter generelle processer og systemopsætninger m.v. hos Complea A/S. Processer og systemopsætninger m.v., der er individuelt aftalt med Compleas kunder er ikke omfattet af erklæringen. Vurdering af eventuelle kundespecifikke processer og systemopsætninger m.v. vil fremgå af specifikke erklæringer til kunder, der har bestilt sådanne.

Kontroller i applikationssystemer er ikke omfattet af denne erklæring.

Complea er en moderne og innovativ virksomhed, som blev grundlagt i 2010 og beskæftiger 50 medarbejdere. Hovedkontoret er placeret i Nørresundby og har ligeledes en filial i Frederikshavn. Tilsvarende tilbyder Complea alle løsninger som Hosted via Compleas eget Hostingcenter. Det betyder, at Complea kan overtage enten hele eller enkelte dele af kunders IT-Løsning. Complea overvåger og tager backup af kunders data 24/7/365, mens kunderne kan fokusere på deres kerneforretning.

Complea betjener kunder over hele Danmark og tilbyder ligeledes support til kundernes udenlandske afdelinger. Målet i Complea er at være Danmarks mest innovative leverandør og servicepartner inden for IT-løsninger, telefoni, ERP-systemer samt softwareudvikling. Ligeledes arbejdes der ud fra en grundfilosofi bestående af fire 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 skal være den markedsledende samarbejdspartner inden for værdiskabende IT- og kommunikationsløsninger baseret på menneskelige værdier… det er os, som markedet kigger på!

***Mission**:* Compleas dedikerede medarbejdere rådgiver, leverer og servicerer værdiskabende IT- og kommunikationsløsninger, der indfrier private og offentlige virksomheders forventninger til teknologi og effektivisering.

Complea sørger for Support og IT drift, så kundernes medarbejdere altid kan arbejde sikkert og effektivt, hvilket sikrer at de kan fokusere 100% på deres kerneforretning.

Complea råder over eget Hostingcenter, som er opbygget efter best-practice og leverer en Hosting ydelse med høj fleksibilitet og stabilitet. Ydelsen 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, 2017 og 2020.

# Generelle IT-kontroller hos Complea A/S

## Indledning

I det følgende beskrives de generelle IT-kontroller relateret til Compleas ydelser til kunder.

### Anvendelse af underleverandører

Complea anvender underleverandørerne GlobalConnect og Norlys i forbindelse med leverancen af netværksforbindelser.

## Risikostyring

Complea har udarbejdet faste procedurer for risikovurdering af forretningen og Hostingcenter. Dette er med henblik på at sikre, at alle risici er minimeret til et acceptabelt niveau, så Complea kan opretholde en normal drift i tilfælde af risici indtræffer.

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

Med udgangspunkt i risikovurderingen og ISO 27002:2013, har Complea udvalgt hovedområder og kontrolmål for styring af it-sikkerheden, der er nærmere beskrevet i det følgende:

## Organisering af it-sikkerheden

Organiseringen af it-sikkerheden sker med udgangspunkt i Compleas IT-sikkerhedspolitik og tager udgangspunkt i ISO 27002:2013, som indeholder følgende hovedområder:

| | | | |
|---|---|---|---|
| 5 | Informationssikkerhedspolitikker | 12 | Driftssikkerhed |
| 6 | Organisering af informationssikkerhed | 13 | Kommunikationssikkerhed |
| 7 | Medarbejdersikkerhed | 14 | Anskaffelse, udvikling og vedligeholdelse af systemer |
| 8 | Styring af aktiver | 15 | Leverandørforhold |
| 9 | Adgangsstyring | 16 | Styring af informations-sikkerhedsbrud |
| 10 | Kryptografi | 17 | Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring |
| 11 | Fysisk sikring og miljøsikring | 18 | Overensstemmelse |

Tilrettelæggelsen af IT-sikkerheden inden for de enkelte områder er beskrevet nedenfor. Kontrolmål og kontroller som Complea har udvalgt, fremgår endvidere af oversigten i afsnit 4.

### Informationssikkerhedspolitikker

Den udarbejdede 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 kontroller, som sikrer at alle udleverede databærende enheder, overholder IT-sikkerhedspolitikken. Der foretages ligeledes overvågning på alt udstyr for at sikre mod installation af uautoriseret software.

### Internet, E-mail og telefoni

I forbindelse med ansættelse 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 ændringerne.

### Data

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

### Videoovervågning

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

## Organisering af informationssikkerhed

Complea har en standard procedure for oprettelse og ansættelse af 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

*IT-sikkerhedsudvalg*
Gennem vidensdeling og efteruddannelse sikrer Complea, at alle medarbejdere efterlever den rolle, som er tiltænkt, samt at alle procedurer fra IT-sikkerhedspolitikken bliver overholdt. Det 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 organisationsudstyr, hvilket dermed også beskytter forretningen.

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

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

*Funktionsadskillelse*
Funktionsadskillelse styres gennem ansættelseskontrakt samt tildeling af adgang til diverse systemer.
Der findes en fast procedure, hvis en medarbejder ønsker udvidelse af eksisterende rettigheder.

## 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.

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

## Medarbejdersikkerhed

Medarbejdersikkerhed stiller krav om tiltag til at reducere risikoen for menneskelige fejl samt misbrug og lignende. Der er udarbejdet en fast procedure for medarbejdersikkerhed før, under, og efter ansættelse i Complea.

### Før ansættelsen

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

*Ansættelsesvilkår og -betingelser*
Vilkår for ansættelse er beskrevet i ansættelseskontrakten hos den enkelte medarbejder. Samtidig udleveres og gennemgås personalehåndbogen ved en af de første arbejdsdage. Det er medarbejderens ansvar at holde sig opdateret på personalehåndbogen. Der gives besked ved ændringer.

### Under ansættelsen

Alle medarbejderdata bliver opbevaret under hele ansættelsesperioden på et netværksdrev, som har opsat begrænset adgang. Der foreligger en fast procedure for at sikre alle medarbejderoplysninger bliver indsamlet og opbevaret korrekt. Der rekvireres årligt en straffeattest på alle medarbejdere i Complea.

*Ledelsesansvar*
Hver medarbejder har en direkte leder i sin afdeling, som sørger for at medarbejderens opgaver og systemadgange er tilsvarende medarbejderens kompetencer og ansættelsesgrundlag. Ligeledes har den nærmeste leder ansvaret for medarbejderens trivsel og at medarbejderen får givet den nødvendige information i dagligdagen.

*Bevidsthed om, uddannelse og træning i informationssikkerhed*
Der foreligger en fast procedure for uddannelse og træning i informationssikkerhed. Dertil bliver alle medarbejdere løbende underrettet og opdateret inden for emnet.

### Ansættelsesforholdets ophør eller ændring

Ved ansættelsesophør bliver alle medarbejderdata 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

Informationssikkerhedspolitikken omfatter alle aktiver, som understøtter Compleas forretningsområder og organisation. Disse omfatter data, systemer, fysiske aktiver samt tekniske forsyninger, der understøtter it-anvendelsen.

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 sikrer 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 de data som Complea har backup af, samtidig med at den kan genskabes, hvis det bliver nødvendigt. Der foreligger 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.

## Ansvar for aktiver

*Fortegnelse over aktiver*
Direktionen har adgang til en fortegnelse over udleverede aktiver til den enkelte medarbejder.

*Ejerskab over aktiver*
I personalehåndbogen står retningslinjerne for ejerskab af aktiver.

*Accepteret brug af aktiver*
Retningslinjerne for accepteret brug af aktiver står beskrevet i personalehåndbogen.

*Tilbagelevering af aktiver*
Jf. proceduren for ansættelsesophør sikres tilbagelevering af aktiver.

## Klassifikation af information

Alle data bliver betragtet som værende fortrolige og medarbejdere har kun 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 evaluering af medarbejderadgange.

## Ny kunde i Hostingcenter

Complea har oprettet en fast procedure for tilknytningen af kunder i Hostingcenter. 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 registreret i Compleas ticketsystem, hvor det er muligt at følge korrespondancen mellem den tildelte tekniker og kunden. Det giver også mulighed for at kontrollere og tjekke sagsforløbet efterfølgende.

Der er udarbejdet en fast procedure, hvis der skal foretages ændringer i Hosting centeret. Alle ændringer bliver dokumenteret af den autoriserede medarbejder i Complea og godkendt af den tekniske direktør.

*Mærkning af information*
Det er kun marketingsmateriale, som ikke bliver betragtet som værende fortroligt.

*Håndtering af aktiver*
Det er kun udvalgte nøglepersoner hos Complea, som har adgang til systemet, der håndterer Hosting. Der foreligger dokumentation for hver kunde, som er hostet. Complea udleverer ikke data til en 3. part eller myndigheder før det er godkendt af direktionen. Samtidig skal en autoriseret medarbejder hos kunden sende en skriftlig henvendelse, hvis Complea skal udlevere data til kundens samarbejdspartner eller leverandør.

## Mediehåndtering

*Styring af flytbare medier*
Da Complea har det overordnede ansvar for flytningen af data sikrer Complea, at der ikke kan forekomme utilsigtet datalæk i forbindelse med flytning af data.

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

*Transport af fysiske medier*
Complea står altid for transporten af databærende udstyr hos eksisterende eller nye kunder.

## Adgangsstyring

Adgangsstyring stiller krav til sikring af adgang til systemer og data. Systemer og data, herunder tekniske basisprogrammer, er sikret mod uberettiget eller utilsigtet adgang. Tildelingen af adgangsrettigheder m.v. sker ud fra et arbejdsbetinget behov og under hensyntagen til en effektiv funktionsadskillelse.

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

### Forretningsmæssige krav til adgangsstyring

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

*Administration af brugeradgange*
Kundens brugeradgang administreres af Complea på baggrund af en skriftlig forespørgsel fra kundens kontaktperson.

*Styring af systemadgange*
Der er udarbejdet en fast procedure til adgangsstyring. Hvis der er et ønske om udvidet adgang skal dette godkendes af den nærmeste leder. Det er et begrænset antal medarbejdere, som har adgang til tildeling af rettigheder.

*Adgang til netværk og netværkstjenester*
Al adgang til kundens systemer foregår via Remote desktopprotokollen eller ved at Complea overtager en PC, som står ved kunden. Således undgår vi at åbne en direkte forbindelse mellem en kundes netværk og Compleas netværk.

## Efteruddannelse og vidensdeling

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

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

## Administration af brugeradgang

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

*Brugerregistrering og – afmelding*
Det er kundens kontaktperson, der står for at sende den skriftlige henvendelse til Complea i forbindelse med forespørgsel på oprettelse af ny bruger. Ligeledes er det også kontaktpersonen, der retter henvendelse, hvis en brugeradgang skal fjernes. Compleas brugeradgang til kundens systemer og data er bestemt af kunden. Der er oprettet en intern procedure for tildeling af rettigheder til Compleas medarbejder.

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

*Styring af privilegerede adgangsrettigheder*
Det er kun ledelsen i Complea, som skal tildele privilegerede adgangsrettigheder.

*Styring af hemmelig autentifikationsinformation om brugere*
Compleas IT-sikkerhedspolitik foreskriver, at medarbejdernes kodeord er personlige og det må ikke deles med andre.

*Gennemgang af brugernes adgangsrettigheder*
Sikkerhed er et nøgleord for Complea og derfor er der lavet en adgangsoversigt, som giver et overblik over adgange for den enkelte medarbejder. Der gennemføres løbende revidering af disse adgange.

*Inddragelse eller justering af adgangsrettigheder*
Brugerens adgangsrettigheder revideres løbende og justeres eller inddrages hvis nødvendigt.

### Brugernes ansvar

*Brug af hemmelig autentifikationsinformation*
Compleas IT-sikkerhedspolitik foreskriver, at medarbejdernes kodeord er personlige og det må ikke deles med andre. Der er opsat en GPO, som sikrer at de foreskrevne retningslinjer overholdes.

### Styring af system- og applikationsadgang

*Begrænset adgang til informationer*
Den enkelte medarbejder er tildelt adgange, så medarbejderen har de fornødne rettigheder til at kunne udføre de opgaver, som medarbejderen er givet.

*Procedurer for sikkert log-on*
Der er opsat 2 faktor godkendelse når der arbejdes udenfor Compleas eget netværk. Adgangen skal godkendes af nærmeste afdelingsleder.

*System for administration af passwords*
Der er opsat en GPO på Compleas netværk, som sikrer alle brugere tilmeldt Compleas domæne overholder de forskrevne retningslinjer for password. I forbindelse med opkobling på kundesystemer registreres der hvilken bruger, der logger på.

*Brug af privilegerede systemprogrammer*
Ledelsen styrer adgangen til privilegerede systemprogrammer.

*Styring af adgang til kildekoder til programmer*
Ledelsen styrer adgangen til *kildekoder til programmer.*

## Kryptografi

### Kryptografiske kontroller

*Politik for anvendelse af kryptografi*
Complea anvender kryptografi til beskyttelse af data og forbindelser.

*Administration af nøgler*
Complea står for administrationen af krypteringsnøgler.

## Fysisk sikring og miljøsikring

Fysisk sikkerhed og miljøsikring omfatter krav og sikkerhedsforanstaltninger til beskyttelse af bygninger, forsyninger og tekniske installationer, der er relevante for Complea.

### Sikre områder

Complea har en adgangsoversigt, som viser hvilke lokationer de enkelte medarbejdere har adgang til. Oversigten bliver løbende revideret.

*Fysisk perimetersikring*
Hovedkontoret er indhegnet og det er ikke muligt at tilgå bygningen uden at blive mødt af Compleas personale i receptionen.

Compleas eget Hostingcenter, som er opført i 2017, er ligeledes indhegnet og kun autoriseret personale har adgang til bygningen. Den adgang bliver gennemgået årligt.

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

*Fysisk adgangskontrol*
Der er installeret tyverialarm på alle Complea filialer og 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 Complea filialer og når en medarbejder benytter sig af sit udleverede adgangskort, bliver det registreret hvornår og hvilken dør medarbejderen benytter. Det gør sig også gældende, hvis der benyttes en dør, hvortil medarbejderen ikke har adgang.

## Sikring af kontorer, lokaler og faciliteter

### *Complea A/S*

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

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

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

*Hosting-underleverandør*
Der foreligger en fast procedure for indhentning af årlig ISAE 3402-II erklæring fra underleverandørerne til hosting-centeret. Disse gennemgås og godkendes af ledelsen.

*Beskyttelse mod eksterne og miljømæssige trusler*
Der er udarbejdet en handlingsplan i Compleas risikoanalyse til håndtering af eksterne og miljømæssige trusler. Ydermere har Complea gjort diverse foranstaltninger for at reducere sandsynligheden for at blive ramt af eksterne og miljømæssige trusler.

## Udstyr

*Placering og beskyttelse af udstyr*
Alle lokationer for Complea er sikret med alarm, videoovervågning og adgangskontrol. Ligeledes er serverrum aflåst og kan kun tilgås af personer, som har særlig adgang.

*Understøttende forsyninger (forsyningssikkerhed)*
Der er opstillet en dieselgenerator med automatisk switch relæ i hovedtavle. De vigtige installationer er beskyttet af et ups anlæg.

*Sikring af kabler*
Kabling er opsat efter best-practice, både indføring og kabling ind i selve hostingcenteret.

*Vedligeholdelse af udstyr*
Der er årlig vedligeholdelse af dieselgeneratoren fra leverandørens side ligesom Complea selv udfører månedlige test på generatoren. Derudover er der implementeret procedure til øvrige vedligeholdelsesopgaver i Hostingcenter.

*Fjernelse af aktiver*
Ledelsen står for fjernelse af aktiver.

*Sikring af udstyr og aktiver uden for organisationens lokaler*
Complea sender data fra Hostingcenter til et brandsikret rum i Hostingcenter ligesom der også bliver sendt en backup til hovedkontoret.

*Sikker bortskaffelse eller genbrug af udstyr*
Al databærende udstyr (USB, CD/DVD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke er tilgængelige. Hvis diske bortskaffes, bliver de fysisk destrueret før de afleveres på en autoriseret genbrugsplads. Hvis en harddisk genbruges, anvendes der autoriseret wipe software, således det sikres, at der ikke kan genskabes indhold på harddisken.

*Brugerudstyr uden opsyn*
I personalehåndbogen er der beskrevet hvordan brugerudstyr skal behandles.

*Politik for ryddeligt udstyr og blank skærm*
I personalehåndbogen er der beskrevet hvordan arbejdspladsen skal se ud efter endt arbejdsdag.

*Driftssikkerhed*
Styring af drift omfatter krav til stabilitet, overvågning og sikkerhed i forbindelse med afvikling af it-produktion. Der er etableret dokumentation af driftsprocesser, driftsafvikling, udstyr og systemer i tilstrækkeligt omfang til, at det muliggør en effektiv driftsafvikling samt en hurtig og effektiv afhjælpning af eventuelle driftsproblemer.

Der kører dagligt en scanning på udstyr, som er logget på Compleas netværk. Det sikrer at uautoriserede programmer ikke er installeret. Der foretages løbende stikprøver for at sikre, at det bliver overholdt.

## Driftsprocedurer og ansvarsområder

*Dokumenterede driftsprocedurer*
Der foreligger en fast procedure for ændringer i Hostingcenter. Alle ændringer er dokumenteret og godkendt af den tekniske direktør. Derudover er der overvågning på alt essentielt udstyr i Hosting og der sendes en alarm, hvis der skulle forekomme uønskede hændelser.

*Ændringsstyring*
Ændringer foretages først, når disse er drøftet, prioriteret og godkendt af ledelsen samt testet efter bedst mulige forhold. Der fastlægges et tidspunkt på, hvornår ændringen kan påbegyndes efter aftale mellem Complea og kunden.

*Kapacitetsstyring*
Complea har opsat overvågning, som giver besked hvis der skal skaleres op af hensyn til elektronisk plads, svartider mv. på både interne og eksterne systemer.

### Patching af systemer

Complea at alle relevante opdateringer, som patches, fixes og servicepacks bliver installeret. Det sikrer at patching af systemer bliver implementeret og kontrolleret, således at systemerne sikres mod nedetid og uautoriseret adgang.

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

*Malwarebeskyttelse*
TrendMicro, som benyttes til malwarebeskyttelse, vil altid været installeret på medarbejdernes PC, 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 forekommer trusler, manglende licenser eller uregelmæssig adfærd.

*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 og overvågning

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

*Beskyttelse af logoplysninger*
Logoplysninger er låst og kan ikke redigeres.

*Administrator- og operatørlogs*
Logning af administratorer sker i forbindelse med den almindelige logning.

*Tidssynkronisering*
Det sikres via domænecontrolleren.

## Styring af driftssoftware

*Softwareinstallation i driftssystemer*
I personalehåndbogen står retningslinjerne for softwareinstallation i driftssystemer. Der er implementeret kontrolprocedure til yderlig kontrol af dette.

## Kommunikationssikkerhed

Netværkssikkerhed omfatter krav til stabilt netværk, hvor datatransmissionen mellem Complea og kunder/samarbejdspartnere er beskyttet mod uautoriseret adgang og utilgængelighed.

Der er udarbejdet en fast procedure for oprettelse af kunder i Hosting. Den bliver gennemgået årligt for at sikre, at den er aktuel og up-to-date.

### Styring af netværkssikkerhed

*Netværksstyring*
Der er firewall installeret foran alle Compleas installationer ligesom der er lavet IP begrænsning (IP-filteret adgang).

*Sikring af netværkstjenester*
Complea installerer firewall på alle installationer og åbner kun for de nødvendige adgange, således at kun godkendt netværkstrafik kan komme gennem firewallen. IT-sikkerhedspolitikken foreskriver hvordan medarbejdere tilgår kunders servere og systemer.

*Opdeling i netværk*
Kunderne er tildelt eget subnet.

## Informationsoverførsel

*Politikker og procedurer for informationsoverførsel*
IT-sikkerhedspolitikken gennemgås i forbindelse med opstart i Complea, således at nye medarbejdere er indforstået med sikkerhedspolitikken.

*Aftaler om informationsoverførsel*
Kundehenvendelser bliver registreret i Compleas ticketsystem. Complea overfører aldrig data til 3. partsvirksomheder uden godkendelse fra kunden. Dette skal godkendes skriftligt fra kunden.

*Elektroniske meddelelser*
Der er opsat elektroniske meddelelser, som bliver afsendt, hvis der forekommer uhensigtsmæssig aktivitet på kundernes netværk.

*Fortroligheds- og hemmeligholdelsesaftaler*
Der er etableret fortrolighed for alle involverede partere i Compleas forretning. Det sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.

## Leverandørforhold

Omfatter informationssikkerhedskravene til at styre risici forbundet med leverandører og outsourcingspartnere.

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

## Informationssikkerhed i leverandørforholdet

*Informationssikkerhedspolitik for leverandørforholdet*
Complea har indgået aftaler med alle underleverandører.

*Håndtering af sikkerhed i leverandøraftaler*
Leverandører vurderes årligt jf. en fastlagt procedure, hvor der indsamles revisorerklæring samt vurdering.

*Forsyningskæde for informations- og kommunikationsteknologi (IKT)*
GlobalConnect og Norlys leverer internetlinjerne til Hostingcenter.

## Styring af leverandørydelser

*Overvågning og gennemgang af leverandørydelser*
Der rekvireres årligt en revisor erklæring fra alle Compleas leverandører, som leverer en driftskritisk ydelse for Complea.

*Styring af ændringer af leverandørydelser*
Såfremt der sker ændringer i Compleas politikker eller procedurer, vurderes det om der er sket ændringer i leverandørforholdet, som skal tilføjes til risikovurdering. På samme måde foregår det, hvis leverandørerne ændrer i deres politikker, procedurer og ydelser.

## Styring af informationssikkerhedsbrud

Information security incident management omfatter krav til kontroller, der skal sikre overblik over indtrufne IT-sikkerhedshændelser samt en hurtig, effektiv og metodisk håndtering af sikkerhedsbrud.

## Styring af informationssikkerhedsbrud og forbedringer

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

*Rapportering af informationssikkerhedshændelser*
Ticketsystemet benyttes til håndtering af størstedelen af alle kundehenvendelser. I ticketsystemet er det muligt at eskalere forhold, således at nogle opgaver får en højere prioritering end andre.

*Rapportering af informationssikkerhedssvagheder*
Medarbejdere og eksterne samarbejdspartnere er forpligtet til at anmelde sikkerhedshændelser til nærmeste leder jf. de indgåede kontrakter, aftaler samt IT-sikkerhedspolitikken. Det skal sikre, at der kan reageres hurtigst muligt på eventuelle hændelser.

*Vurdering af og beslutning om informationssikkerhedshændelser*
Relevante medarbejdere vurderer de indkomne opgaver og løser opgaverne hurtigst muligt efter vigtighedsprioritering. Der er opsat procedurer for eskalering af opgaver

*Håndtering af informationssikkerhedsbrud*
I tilfælde af sikkerhedssvagheder vil direktionen blive informeret og nødvendige tiltag for at reducere hændelsen vil finde sted hurtigst muligt. Ved større hændelser aktiveres Compleas beredskabsplan.

*Erfaring fra informationssikkerhedsbrud*
I tilfælde af nedbrud, vil der blive foretaget en evaluering efterfølgende, for at undgå samme problematik fremadrettet.

*Indsamling af beviser*
IT-beredskabsplanen forskriver hvordan beviser skal indsamles i tilfælde af et sikkerhedsbrud.

## Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Omfatter krav til beredskabsstyring, herunder udarbejdelse og test af beredskabsplaner.

## Informationssikkerhedskontinuitet

*Planlægning af informationssikkerhedskontinuitet*
Der er udarbejdet en IT-beredskabsplan i tilfælde af sikkerhedsbrud. Alle involverede parter er informeret om deres rolle, hvis der skulle forekomme en hændelse som kræver at beredskabsplanen aktiveres. Beredskabsplanen godkendes af ledelsen og testes årligt.

*Implementering af informationssikkerhedskontinuitet*
Beredskabsplanen er udleveret til de medarbejdere, som indgår i IT-beredskabet, således at de involverede medarbejdere altid har IT-beredskabsplanen til rådighed.

*Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten*
Der foretages årlig skrivebordstest af IT-beredskabsplanen, som verificeres, gennemgås og evalueres. Ligeledes er der en fast procedure for afprøvning af hele IT-beredskabsplanen.

## Redundans

*Tilgængelighed af informationsbehandlingsfaciliteter*
Der er overvågning og lavet redundans på alt driftskritisk udstyr i Hostingcenter

## Overensstemmelse

Overensstemmelse stiller krav til kontroller til sikring mod brud på relevante IT-sikkerhedskrav.

## Gennemgang af informationssikkerhed

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.

*Uafhængig 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.

*Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder*
Sikkerhedspolitikker og sikkerhedsstandarder gennemgås og revideres årligt, så Complea altid kan stå inde for den højeste sikkerhed både internt og eksternt.

*Undersøgelse af teknisk overensstemmelse*
Der foretages løbende undersøgelser for at sikre at udstyr, software osv. som overholder kravene ift. efterlever sikkerhedskravet i Complea.

## Væsentlige ændringer i it-miljøerne

Der er ikke gennemført væsentlige ændringer i it-anvendelsen eller kontrolmiljøet i perioden 1. januar 2021 til 31. december 2021.

## Komplementerende kontroller hos kunderne

Kontrollerne hos Complea er udformet sådan, at nogle af kontrollerne nævnt i denne erklæring skal suppleres med kontroller hos kunderne. Nedenstående kontroller forventes implementeret og udført hos og af kunderne for at opfylde de kontrolmål, der er anført i denne rapport. Nedenstående oplistning af komplementerende kontroller hos kunderne skal ikke betragtes som en udtømmende oplistning af kontroller, der bør implementeres af og udføres hos kunderne.

Compleas kunder er, medmindre andet er aftalt, ansvarlige for:

- At der foretages 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.
- At internet, som ikke er leveret af Complea er funktionelt.

# Afsnit 2: Complea A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Complea A/S' hosting-platform, 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 anvender serviceunderleverandørerne Global Connect A/S og Nordlys A/S. Denne erklæring er udarbejdet efter partielmetoden, og Complea A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Serviceunderleverandørerne Global Connect A/S og Nordlys A/S.

Complea A/S bekræfter, at:

(a) Den medfølgende beskrivelse i afsnit 1, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Complea A/S' hosting-platform, der har behandlet kunders transaktioner i perioden fra 1. januar 2021 til 31. december 2021.

Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været udformet og implementeret, herunder redegør for:
- De typer af ydelser, der er leveret.
- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål og kontroller udformet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes 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 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 de generelle it-kontroller.

(ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget i perioden fra 1. januar 2021 til 31. december 2021

(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 perioden fra 1. januar 2021 til 31. december 2021. Kriterierne for denne udtalelse var, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar 2021 til 31. december 2021.

Nørresundby, den 10. februar 2022
Complea A/S

Morten Hovaldt
CEO

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

Til Complea A/S, deres kunder, og deres revisorer.

## Omfang

Vi har fået som opgave at afgive erklæring om Complea A/S' beskrivelse i afsnit 1 af generelle it-kontroller for drift af brugersystemer til behandling af Complea A/S' kunders transaktioner i perioden 1. januar 2021 til 31. december 2021 og om udformningen og funktionaliteten af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Complea A/S anvender serviceunderleverandørerne Global Connect A/S og Nordlys A/S. Denne erklæring er udarbejdet efter partielmetoden, og Complea A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Global Connect A/S og Nordlys A/S.

Enkelte af de kontrolmål, der er anført i Complea A/S' beskrivelse i afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne (eller den specifikke kunde) er hensigtsmæssigt udformet og fungerer effektivt sammen med kontrollerne hos Complea A/S. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

## Complea A/S' ansvar

Complea A/S er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 1) og tilhørende udtalelse (afsnit 2), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og 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 International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

REVI-IT anvender ISQC 1[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.

[1] ISQC 1, Kvalitetsstyring i firmaer, som udfører revision og review af regnskaber, andre erklæringsopgaver med sikkerhed og beslægtede opgaver.

## REVI-IT A/S' ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Complea A/S' beskrivelse (afsnit 1) og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning.

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.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af 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 udformet 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 desuden 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 Complea A/S' udtalelse 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 1 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 de generelle it-kontroller, som hver enkelt kunde måtte anse for vigtigt efter deres 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. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i Complea A/S' udtalelse i afsnit 2.

Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var udformet og implementeret i perioden 1. januar 2021 til 31. december 2021, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden fra 1. januar 2021 til 31. december 2021
(c) 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 perioden 1. januar 2021 til 31. december 2021.

## 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 afsnit 4 om kontrolmål, udførte kontroller, test og resultater heraf.

## Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt Complea A/S' hosting-platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 10. februar 2022

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Partner, CISA

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

## 4.1. Formål og omfang

Beskrivelse og resultat af vores tests af kontroller fremgår af efterfølgende skema. I det omfang vi ved vores test har konstateret afvigelser i design, implementering eller operationel effektivitet af de testede kontroller, har vi anført disse under resultat af test.

Denne erklæring er udarbejdet efter partielmetoden og Complea A/S' kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos Complea A/S' underleverandør Global Connect A/S og Nordlys A/S.

Kontroller udført hos Complea A/S' kunder, er ikke omfattet af vores erklæring.

## 4.2. Udførte test

Metoder anvendt til test af kontrollers funktionalitet er beskrevet nedenfor:

| Metode | Overordnet beskrivelse |
|---|---|
| Forespørgsel | Forespørgsel af passende personale hos Complea A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres. |
| Observation | Observation af, hvordan kontroller udføres. |
| Inspektion | Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. |
| Genudførelse af kontrol | Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat. |

## 4.3. Resultater af test

I nedenstående oversigt har vi opsummeret tests udført af REVI-IT som grundlag for vurdering af de generelle it-kontroller hos Complea A/S.

### A.4 Risikovurdering og -håndtering

Risikovurdering
Kontrolmål: At sikre, at virksomheden regelmæssigt foretager en analyse og vurdering af it-risikobilledet.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 4.1 | Complea A/S' sikkerhedsprogram er struktureret omkring 3 primære aktiviteter: Risikovurdering, risikohåndtering og løbende monitorering. Risikovurdering er en gennemgående og kontinuerlig opgave. Der udføres årligt et antal risikoanalyser.<br><br>Efter verifikation og klassifikation dokumenteres de fundne risici i Complea A/S' risikoregister. Her dokumenteres også hvilke initiativer, der er igangsat for at reducere eller imødegå de enkelte risici. Status på risici rapporteres månedligt til Complea A/S' ledelse.<br><br>I forbindelse med leverancer foretages der risikovurdering under udarbejdelsen af tilbud. | Vi har forespurgt til udarbejdelsen af en risikoanalyse, og vi har inspiceret den udarbejdede risikoanalyse.<br><br>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 perioden. | Ingen afvigelser konstateret. |

## A.5 Informationssikkerhedspolitikker

### A.5.1 Retningslinjer for styring af informationssikkerhed

Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 5.1.1 | *Politikker for informationssikkerhed*<br><br>Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter. | Vi har observeret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejdere. | Ingen afvigelser konstateret. |
| 5.1.2 | *Gennemgang af politikker for informationssikkerhed*<br><br>Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet. | Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken.<br><br>Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv. | Ingen afvigelser konstateret. |

## A.6 Organisering af informationssikkerhed

A.6.1 Intern organisering
Kontrolmål: At etablere 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 |
|---|---|---|---|
| 6.1.1 | *Roller og ansvarsområder for informationssikkerhed*<br><br>Alle ansvarsområder for informationssikkerhed defineres og fordeles. | Vi har inspiceret dokumentation, der viser, at ansvaret for informationssikkerhed er klart defineret og fordelt. | Ingen afvigelser konstateret. |
| 6.1.2 | *Funktionsadskillelse*<br><br>Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver. | Vi har inspiceret procedurer vedrørende tildeling og opretholdelse af adskillelse af ansvarsområder og funktioner.<br><br>Ved forespørgsel og inspektion af systemudtræk har vi undersøgt om driftspersonale kun har adgang til at administrere rettigheder på systemer, for hvilke de er ansvarlige. | Ingen afvigelser konstateret. |
| 6.1.3 | *Kontakt med myndigheder*<br><br>Der opretholdes passende kontakt med relevante myndigheder. | Vi har inspiceret proceduren vedrørende vedligeholdelse af reglerne for passende kontakt med relevante myndigheder. | Ingen afvigelser konstateret. |
| 6.1.4 | *Kontakt med særlige interessegrupper*<br><br>Der opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer. | Vi har inspiceret proceduren vedrørende vedligeholdelse af reglerne for passende kontakt med særlige interessegrupper, faglige sikkerhedsfora og faglige organisationer. | Ingen afvigelser konstateret. |
| 6.1.5 | *Informationssikkerhed ved projektstyring*<br><br>Informationssikkerhed anvendes ved projektstyring, uanset projekttype. | Vi har observeret, om der i projekter, i passende omfang, tages stilling til it-sikkerhedsmæssige forhold. | Ingen afvigelser konstateret. |

| A.6.2 Mobilt udstyr og fjernarbejdspladser<br>Kontrolmål: Formålet er at sikre fjernarbejdspladser og brugen af mobilt udstyr. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 6.2.1 | *Politik for mobilt udstyr*<br><br>Der vedtages en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr. | Vi har inspiceret politik for sikring af mobile enheder.<br><br>Vi har inspiceret, at der er defineret tekniske kontroller til sikring af mobile enheder.<br><br>Vi har inspiceret, at tekniske kontroller er implementeret på mobile enheder. | Ingen afvigelser konstateret. |
| 6.2.2 | *Fjernarbejdspladser*<br><br>Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser. | Vi har inspiceret politik for sikring af fjernarbejdspladser, og vi har inspiceret underliggende sikkerhedsforanstaltninger til beskyttelse af fjernarbejdspladser. | Ingen afvigelser konstateret. |

## A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen
Kontrolmål: Formålet er at sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er tiltænkt.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 7.1.1 | *Screening*<br><br>Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse se med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici. | Vi har inspiceret proceduren for ansættelse af nye medarbejdere og de sikkerhedsopgaver, der skal udføres i den forbindelse.<br><br>Vi har inspiceret et udvalg af ansættelsesaftaler med henblik på at konstatere, om proceduren med hensyn til baggrundscheck efterleves for nye medarbejdere. | Ingen afvigelser konstateret. |
| 7.1.2 | *Ansættelsesvilkår og -betingelser*<br><br>Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed. | Vi har inspiceret et udvalg af kontrakter med medarbejdere med henblik på at konstatere om medarbejdere havde underskrevet kontrakten. | Ingen afvigelser konstateret. |

| A.7.2 Under ansættelsen<br>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** |
| 7.2.1 | *Ledelsesansvar*<br><br>Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer. | Vi har inspiceret proceduren vedrørende fastsættelse af krav til medarbejdere og kontrahenter.<br><br>Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde it-sikkerhedspolitikken. | Ingen afvigelser konstateret. |
| 7.2.2 | *Bevidsthed om, uddannelse og træning i informationssikkerhed*<br><br>Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter vil ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, idet omfang det er relevant for deres jobfunktion. | Vi har inspiceret procedurer til sikring af tilstrækkelig uddannelse og træning (awarenesstræning).<br><br>Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejdere. | Ingen afvigelser konstateret. |
| 7.2.3 | *Sanktioner*<br><br>Der etableres en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud. | Vi har inspiceret, at der er etableret en formel sanktionsproces, som er kommunikeret til medarbejderne. | Ingen afvigelser konstateret. |

| A.7.3 Ansættelsesforholdets ophør eller ændring<br>Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 7.3.1 | *Ansættelsesforholdets ophør eller ændring*<br><br>Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves. | Vi har forespurgt til medarbejderes og kontrahenters forpligtelser til opretholdelse af informationssikkerhed i forbindelse med ophør af ansættelse eller kontrakt.<br><br>Vi har inspiceret dokumentation for at informationssikkerhedsansvar og -forpligtelser er defineret og kommunikeret. | Ingen afvigelser konstateret. |

## A.8 Styring af aktiver

A.8.1 Ansvar for aktiver
Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 8.1.1 | *Fortegnelse over aktiver*<br><br>Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver. | Vi har inspiceret fortegnelser over aktiver. | Ingen afvigelser konstateret. |
| 8.1.2 | *Ejerskab af aktiver*<br><br>Der udpeges en ejer i organisationen for hvert aktiv. | Vi har inspiceret oversigt over ejerskab til aktiver. | Ingen afvigelser konstateret. |
| 8.1.3 | *Accepteret brug af aktiver*<br><br>Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, dokumenteres og implementeres. | Vi har inspiceret reglerne for accepteret brug af aktiver. | Ingen afvigelser konstateret. |
| 8.1.4 | *Tilbagelevering af aktiver*<br><br>Alle medarbejdere og eksterne brugere afleverer alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører. | Vi har inspiceret proceduren til sikring af tilbagelevering af udleverede aktiver.<br><br>Vi har forespurgt om udleverede aktiver inddrages. | Ingen afvigelser konstateret. |

## A.9 Adgangsstyring

### A.9.1 Forretningsmæssige krav til adgangsstyring
Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 9.1.1 | *Politik for adgangsstyring*<br><br>En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav. | Vi har inspiceret politikken for adgangsstyring med henblik på at konstatere, om den var opdateret og godkendt. | Ingen afvigelser konstateret. |

| A.9.2 Administration af brugeradgang<br>Kontrolmål: 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** |
| 9.2.1 | *Brugerregistrering-og afmelding*<br>Der implementeres en formel procedure for registrering og afmelding af brugere med henblik på tildeling af adgangsrettigheder. | Vi har forespurgt til procedurer for registrering og afmelding af brugere, og vi har inspiceret procedurerne.<br>Vi har inspiceret et udvalg af registrering og afmelding af brugere. | Ingen afvigelser konstateret. |
| 9.2.2 | *Tildeling af brugeradgang*<br>Der implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester. | Vi har inspiceret, at der er etableret en procedure for brugeradministration.<br>Vi har inspiceret, at proceduren for brugeradministration er implementeret. | Ingen afvigelser konstateret. |
| 9.2.3 | *Styring af privilegerede adgangsrettigheder*<br>Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres. | Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder.<br>Vi har inspiceret et udvalg af privilegerede brugere for at konstatere om processen er blevet overholdt. | Ingen afvigelser konstateret. |
| 9.2.4 | *Styring af hemmelig autentifikationsinformation om brugere*<br>Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces. | Vi har inspiceret proceduren vedrørende tildeling af passwords til platforme.<br>Vi har for et udvalg af tildelinger af passwords inspiceret, at proceduren overholdes. | Ingen afvigelser konstateret. |
| 9.2.5 | *Gennemgang af brugeradgangsrettigheder*<br>Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder. | Vi har inspiceret proceduren for regelmæssig gennemgang og evaluering af adgangsrettigheder.<br>Vi har inspiceret et udvalg af gennemgang og evalueringer af adgangsrettigheder. | Ingen afvigelser konstateret. |

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 9.2.6 | *Inddragelse eller justering af adgangsrettigheder*<br><br>Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring. | Vi har inspiceret procedurerne for inddragelse og justering af adgangsrettigheder.<br><br>Vi har, for et udvalg af fratrådte medarbejdere, inspiceret hvorvidt medarbejderne har fået deres adgangsrettigheder inddraget. | Ingen afvigelser konstateret. |

| A.9.3 Brugernes ansvar<br>Kontrolmål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 9.3.1 | *Brug af hemmelig autentifikationsinformation*<br><br>Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation. | Vi har inspiceret retningslinjer for brug af fortrolige passwords. | Ingen afvigelser konstateret. |

| A.9.4 Styring af system- og applikationsadgang<br>Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 9.4.2 | *Procedurer for sikker logon*<br>Adgang til systemer og applikationer styres af en procedure for sikker logon. | Vi har forespurgt til proceduren for sikkert logon, og vi har inspiceret den implementerede løsning. | Ingen afvigelser konstateret. |
| 9.4.3 | *System for administration af passwords*<br>Systemer til administration af passwords er interaktive og sikrer passwords med god kvalitet. | Vi har inspiceret, at der i politikker eller procedurer stilles krav til kvaliteten af passwords.<br>Vi har inspiceret at systemer til administration af passwords er opsat i overensstemmelse med de stillede krav. | Ingen afvigelser konstateret. |

## A.10 Kryptografi

A.10.1 Kryptografiske kontroller
Kontrolmål: 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 |
|---|---|---|---|
| 10.1.1 | *Politik for anvendelse af kryptografi*<br><br>Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information. | Vi har forespurgt til politik for anvendelse af kryptering, og vi har stikprøvevis inspiceret brugen af kryptografi. | Ingen afvigelser konstateret. |
| 10.1.2 | *Administration af nøgler*<br><br>Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus. | Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker.<br><br>Vi har stikprøvevis inspiceret, at der er dokumentation for, at de anvendte teknikker er anvendt som beskrevet. | Ingen afvigelser konstateret. |

## A.11 Fysisk sikring og miljøsikring

A.11.1 Sikre områder
Kontrolmål: 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 |
|---|---|---|---|
| 11.1.1 | *Fysisk perimetersikring*<br>Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter. | Vi har inspiceret proceduren for fysisk beskyttelse af faciliteter og perimetersikkerhed.<br>Vi har inspiceret relevante lokationer og deres perimetersikring for at konstatere, hvorvidt der er sikringsforanstaltninger til at forhindre uautoriseret adgang. | Ingen afvigelser konstateret. |
| 11.1.2 | *Fysisk adgangskontrol*<br>Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang. | Vi har inspiceret procedurerne for adgangskontrol til sikre områder.<br>Vi har inspiceret udvalgte adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til produktionsfaciliteterne. | Ingen afvigelser konstateret. |
| 11.1.3 | *Sikring af kontorer, lokaler og faciliteter*<br>Fysisk sikring af kontorer, lokaler og faciliteter er tilrettelagt og etableret. | Vi har stikprøvevis inspiceret, at der er etableret fysisk sikring af kontorer, lokaler og faciliteter.<br>Vi har inspiceret, at der foretages inspektion af brandsluknings-udstyr og UPS-anlæg m.v.<br>Vi har inspiceret, at der gennemføres test af generatorer, UPS-anlæg m.v. | Ingen afvigelser konstateret. |
| 11.1.4 | *Beskyttelse mod eksterne og miljømæssige trusler*<br>Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret. | Vi har inspiceret proceduren vedrørende beskyttelse mod eksterne og miljømæssige trusler.<br>Vi har forespurgt om implementering af sikkerhedsforanstaltninger til at forhindre trusler fra ild, varme og fugt og inspiceret relevante lokationer for at konstatere, om der er installeret brandslukningsudstyr, brand- og røgalarmer. | Ingen afvigelser konstateret. |

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 11.1.5 | *Arbejde i sikre områder*<br><br>Procedurer for arbejde i sikre områder er tilrettelagt og etableret. | Vi har inspiceret procedurer for arbejde i sikre områder. | Ingen afvigelser konstateret. |

| A.11.2 Udstyr<br>Kontrolmål: 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** |
| 11.2.1 | *Placering og beskyttelse af udstyr*<br><br>Udstyr er placeret og beskyttet, så risikoen for miljøtrusler og farer samt for muligheden for uautoriseret adgang nedsættes. | Vi har inspiceret proceduren vedrørende placering og beskyttelse af udstyr.<br><br>Vi har inspiceret relevante lokationer for at vurdere, hvorvidt lokaler er sikkert aflåst og kontrolleret, og at kun medarbejdere med et arbejdsbetinget behov har adgang hertil. | Ingen afvigelser konstateret. |
| 11.2.2 | *Understøttende forsyninger (forsyningssikkerhed)*<br><br>Udstyr er beskyttet mod strømsvigt og andre forstyrrelser som følge af svigt af understøttende forsyninger. | Vi har inspiceret proceduren for beskyttelse af udstyr mod strømafbrydelser og andre afbrydelser som følge af svigt i understøttende forsyninger.<br><br>Vi her inspiceret at backupstrøm, UPS-anlæg og dieselgeneratorer med tilstrækkelig kapacitet har været til rådighed.<br><br>Vi har inspiceret servicerapporter, der viser, at serviceinspektioner er udført i overensstemmelse med leverandørers anbefalinger, og at udstyr testes regelmæssigt. | Ingen afvigelser konstateret. |

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 11.2.3 | *Sikring af kabler*<br><br>Kabler til elektricitet og telekommunikation, som bærer data eller understøtter informationstjenester, er beskyttet mod indgreb, interferens og skader. | Vi har inspiceret beskyttelsen af et udvalg af strøm- og datakabler med henblik på at konstatere om kablerne var beskyttet mod indgreb og skader. | Ingen afvigelser konstateret. |
| 11.2.6 | *Sikring af udstyr og aktiver uden for organisationen*<br><br>Der er etableret sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen. | Vi har inspiceret retningslinjer for sikring af udstyr og aktiver uden for organisationen. | Ingen afvigelser konstateret. |
| 11.2.7 | *Sikker bortskaffelse eller genbrug af udstyr*<br><br>Alt udstyr med lagringsmedier verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug. | Vi har inspiceret proceduren for sletning af data og software på lagringsmedier inden bortskaffelse af lagringsmediet.<br><br>Vi har inspiceret bortskaffelse af et udvalg af udstyr med henblik på at konstatere, om data og software blev slettet inden bortskaffelsen fandt sted. | Ingen afvigelser konstateret. |
| 11.2.8 | *Brugerudstyr uden opsyn*<br><br>Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet. | Vi har inspiceret proceduren for sikring af beskyttelse af udstyr, som er uden opsyn. | Ingen afvigelser konstateret. |
| 11.2.9 | *Politik for ryddeligt skrivebord og blank skærm*<br><br>Der er udarbejdet en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter. | Vi har inspiceret politik for ryddeligt skrivebord og blank skærm. | Ingen afvigelser konstateret. |

## A.12 Driftssikkerhed

A.12.1 Driftsprocedurer og ansvarsområder
Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 12.1.1 | *Dokumenterede driftsprocedurer*<br><br>Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem. | Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret og vedligeholdt.<br><br>Vi har stikprøvevis inspiceret, at driftsdokumentation er opdateret og tilgængelig for medarbejdere, som har behov for dem. | Ingen afvigelser konstateret. |
| 12.1.2 | *Ændringsstyring*<br><br>Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres. | Vi har inspiceret proceduren vedrørende ændringer til informationsbehandlingsudstyr og – systemer.<br><br>Vi har inspiceret, at et udvalg af ændringer foretaget på platforme, databaser og netværksudstyr er godkendt, testet, dokumenteret og implementeret i produktionsmiljøet i overensstemmelse med Change Management proceduren. | Ingen afvigelser konstateret. |
| 12.1.3 | *Kapacitetsstyring*<br><br>Anvendelsen af ressourcer overvåges og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet. | Vi har inspiceret proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav.<br><br>Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring. | Ingen afvigelser konstateret. |

| A 12.2 Malwarebeskyttelse<br>Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 12.2.1 | *Kontroller mod malware*<br><br>Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed. | Vi har forespurgt til foranstaltninger mod malware.<br><br>Vi har forespurgt til anvendelsen af antivirusprogrammer, og vi har inspiceret dokumentation for anvendelsen. | Ingen afvigelser konstateret. |

| A.12.3 Backup<br>Kontrolmål: At beskytte mod tab af data. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 12.3.1 | *Backup af information*<br><br>Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik. | Vi har forespurgt til krav til konfiguration af backup, og vi har stikprøvevis inspiceret dokumentation for, at opsætningen var i overensstemmelse med kravene.<br><br>Vi har inspiceret, at der gennemføres overvågning af afviklingen af backup.<br><br>Vi har forespurgt til test af gendannelse fra backupfiler, og vi har inspiceret dokumentation for test af gendannelse. | Ingen afvigelser konstateret. |

| A.12.4 Logning og overvågning<br>Kontrolmål: At registrere hændelser og tilvejebringe bevis. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 12.4.1 | *Hændelseslogning*<br>Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt. | Vi har forespurgt til logning af brugeraktivitet.<br>Vi har stikprøvevis inspiceret logningskonfigurationerne. | Ingen afvigelser konstateret. |
| 12.4.2 | *Beskyttelse af log- oplysninger*<br>Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang. | Vi har forespurgt til procedurer for sikring af logoplysninger.<br>Vi har inspiceret et udvalg af logningskonfigurationer med henblik på at konstatere, om logningsinformationer er beskyttet mod manipulation og uautoriseret adgang. | Ingen afvigelser konstateret. |
| 12.4.3 | *Administrator- og operatørlog*<br>Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt. | Vi har inspiceret procedurer vedrørende logning af aktiviteter udført af systemadministratorer og -operatører.<br>Vi har inspiceret logopsætninger på udvalgte servere og databasesystemer med henblik på at konstatere, om systemadministratorers og -operatørers handlinger logges. | Ingen afvigelser konstateret. |
| 12.4.4 | *Tidssynkronisering*<br>Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne er synkroniserede til en enkelt referencetidskilde. | Vi har forespurgt til proceduren for synkronisering op imod en betryggende tidsserver, og vi har inspiceret løsningen. | Ingen afvigelser konstateret. |

| A.12.5 Styring af driftssoftware<br>Kontrolmål: At sikre integriteten af driftssystemer. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 12.5.1 | *Softwareinstallation på driftssystemer*<br>Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer. | Vi har inspiceret retningslinjer for installation af software på driftssystemer, og vi har stikprøvevis inspiceret, at retningslinjerne efterleves. | Ingen afvigelser konstateret. |

| A.12.6 Sårbarhedsstyring<br>Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 12.6.1 | *Styring af tekniske sårbarheder*<br><br>Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko. | Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder.<br><br>Vi har stikprøvevis inspiceret servere, databasesystemer og netværkskomponenter for at konstatere, hvorvidt de er patchet rettidigt. | Ingen afvigelser konstateret. |
| 12.6.2 | *Begrænsninger på softwareinstallation*<br><br>Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne. | Vi har forespurgt til procedurer for begrænsning af softwareinstallation, som foretages af brugere.<br><br>Vi har inspiceret, at regler for softwareinstallation efterleves. | Ingen afvigelser konstateret. |

## A.13 Kommunikationssikkerhed

### A.13.1 Styring af netværkssikkerhed

Kontrolmål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 13.1.1 | *Netværksstyring*<br><br>Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer. | Vi har inspiceret, at der er defineret krav om styring og kontrol af netværk, herunder krav og regler om kryptering, segmentering, firewalls, intrusion detection og andre relevante sikkerhedsforanstaltninger.<br><br>Vi har inspiceret dokumentation for design af netværket og et udvalg af sikkerhedsmæssige opsætninger af netværkskomponenter med henblik på at konstatere, om de definerede krav og regler er implementerede. | Ingen afvigelser konstateret. |
| 13.1.2 | *Sikring af netværkstjenester*<br><br>Sikkerhedsmekanismer, serviceniveauer og styringskrav til alle netværkstjenester identificeres og indgår i aftaler om netværkstjenester, uanset om disse tjenester leveres internt eller er outsourcede. | Vi har observeret, at der foreligger skriftlige krav til sikkerhedsmekanismer, serviceniveauer og styringskrav til netværkstjenester.<br><br>Vi har inspiceret et udvalg af netværkskomponenter for at vurdere, hvorvidt komponenterne er opsat i overensstemmelse med kravene og leverandørernes anbefalede baselines. | Ingen afvigelser konstateret. |
| 13.1.3 | *Opdeling af netværk*<br><br>Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk. | Vi har inspiceret retningslinjerne for segmentering af netværk.<br><br>Vi har inspiceret et udvalg af adgange mellem netværkszoner med hensyn til, om de er begrænset til nødvendige tjenester. | Ingen afvigelser konstateret. |

| A.13.2 Informationsoverførsel<br>Kontrolmålet: 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** |
| 13.2.1 | *Politikker og procedurer for informationsoverførsel*<br><br>Der foreligger formelle politikker, procedurer og kontroller for overførsel for at beskytte informationsoverførsel ved brug af alle former for kommunikationsudstyr. | Vi har inspiceret politikker og procedurer for dataoverførsel. | Ingen afvigelser konstateret. |
| 13.2.3 | *Elektroniske meddelelser*<br><br>Informationer i elektroniske meddelelser beskyttes på passende måde. | Vi har forespurgt til retningslinjer for afsendelse af fortrolig information. | Ingen afvigelser konstateret. |
| 13.2.4 | *Fortroligheds- og hemmeligholdelsesaftaler*<br><br>Krav til fortroligheds- og hemmeligholdelsesaftaler, der afspejler organisationens behov for at beskytte information, identificeres, gennemgås regelmæssigt og dokumenteres. | Vi har forespurgt til proceduren for etablering af fortrolighedsaftaler.<br><br>Vi har inspiceret et udvalg af underskrevne fortrolighedsaftaler med henblik på at konstatere, om proceduren efterleves ved ansættelse af nye medarbejdere og indgåelse af aftaler med konsulenter. | Ingen afvigelser konstateret. |

## A.15 Leverandørforhold

15.2 Styring af leverandørydelser

Kontrolmål: 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 |
|---|---|---|---|
| 15.2.1 | *Overvågning og gennemgang af leverandørydelser*<br>Organisationer overvåger, gennemgår og auditerer leverandørydelser. | Vi har inspiceret proceduren for overvågning og gennemgang af serviceydelser leveret af underleverandører er i overensstemmelse med det aftalte.<br>Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører. | Ingen afvigelser konstateret. |
| 15.2.2 | *Styring af ændringer af leverandørydelser*<br>Leverandørydelser overvåges, gennemgås og auditeres. | Vi har forespurgt til styring af ændringer hos leverandører og har inspiceret retningslinjer for håndtering af ændringer. | Vi er blevet informeret om, at der ikke har været væsentlige ændringer til leverandørydelser i perioden, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen.<br>Ingen afvigelser konstateret. |

## A.16 Styring af informationssikkerhedsbrud

A.16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: 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 |
|---|---|---|---|
| 16.1.1 | *Ansvar og procedurer*<br>Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud. | Vi har forespurgt til ansvar og procedurer i forbindelse med informationssikkerhedshændelser, og vi har inspiceret dokumentation for ansvarsfordeling.<br>Vi har endvidere inspiceret proceduren til håndtering af informationssikkerhedshændelser. | Ingen afvigelser konstateret. |
| 16.1.2 | *Rapportering af informationssikkerhedshændelser*<br>Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt. | Vi har forespurgt til retningslinjer for rapportering af informationssikkerhedshændelser og -svagheder, og vi har inspiceret retningslinjerne. | Ingen afvigelser konstateret. |
| 16.1.3 | *Rapportering af informationssikkerhedssvagheder*<br>Medarbejdere og kontrahenter, som bruger organisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observerede svagheder eller mistanke om svagheder i informationssystemer og -tjenester. | Vi har forespurgt til informationssikkerhedshændelser i perioden, og vi har forespurgt til dokumentation for håndtering af disse. | Vi er blevet informeret om, at der ikke har været informationssikkerhedshændelser i perioden, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen.<br>Ingen afvigelser konstateret. |
| 16.1.4 | *Vurdering af og beslutning om informations- sikkerhedshændelser*<br>Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som informationssikkerhedsbrud. | Vi har inspiceret proceduren for vurdering og evaluering af informationssikkerhedsbrud. | Vi er blevet informeret om, at der ikke har været informationssikkerhedshændelser i perioden, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen.<br>Ingen afvigelser konstateret. |
| 16.1.5 | *Håndtering af informationssikkerhedsbrud*<br>Informationssikkerhedsbrud håndteres i overensstemmelse se med de dokumenterede procedurer. | Vi har forespurgt til, at informationssikkerhedsbrud har været håndteret i overensstemmelse med de dokumenterede procedurer. | Vi er blevet informeret om, at der ikke har været informationssikkerhedsbrud, hvorfor det ikke har været muligt at teste effektiviteten af kontrollen.<br>Ingen afvigelser konstateret. |

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 16.1.6 | *Erfaring fra informationssikkerhedsbrud*<br><br>Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud. | Vi har forespurgt vedrørende Problem Management-funktion, der analyserer informationssikkerhedsbrud med henblik på at reducere sandsynligheden for at de gentager sig. | Ingen afvigelser konstateret. |

## A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

A.17.1 Informationssikkerhedskontinuitet
Kontrolmål: 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 |
|---|---|---|---|
| 17.1.1 | *Planlægning af informationssikkerhedskontinuitet*<br><br>Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe. | 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. | Ingen afvigelser konstateret. |
| 17.1.2 | *Implementering af informationssikkerheds- kontinuitet*<br><br>Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes. | Vi har forespurgt om der er procedurer der sikrer, at alle relevante systemer indgår i beredskabsplanlægningen.<br><br>Vi har inspiceret om beredskabsplanen vedligeholdes. | Ingen afvigelser konstateret. |

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 17.1.3 | *Verificer, gennemgå og evaluer informations- sikkerhedskontinuiteten*<br><br>Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer. | Vi har forespurgt til test af beredskabsplanen, og vi har inspiceret dokumentation for udført test.<br><br>Vi har endvidere forespurgt til regelmæssig revurdering af beredskabsplanen, og vi har inspiceret dokumentation for revurderingen. | Ingen afvigelser konstateret. |

| A.17.2 Redundans<br>Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter. | | | |
|---|---|---|---|
| **Nr.** | **Complea A/S' kontrol** | **REVI-IT's test** | **Resultat af test** |
| 17.2.1 | Tilgængelighed af informationsbehandlingsfaciliteter<br><br>Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav. | Vi har forespurgt til etablering af redundans til sikring af tilgængelighed af driftssystemer, og vi har inspiceret de etablerede foranstaltninger. | Ingen afvigelser konstateret. |

## A.18 Overensstemmelse

### A.18.2 Gennemgang af informationssikkerheden

Kontrolmål: 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 |
|---|---|---|---|
| 18.2.1 | *Uafhængig gennemgang af informationssikkerhed*<br><br>Organisationens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer. | Vi har observeret, at der er etableret krav om regelmæssig uafhængig revisionsmæssig gennemgang af informationssikkerheden. | Ingen afvigelser konstateret. |
| 18.2.2 | *Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder*<br><br>Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav. | Vi har forespurgt vedrørende lederes sikring af overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder. | Ingen afvigelser konstateret. |

| Nr. | Complea A/S' kontrol | REVI-IT's test | Resultat af test |
|---|---|---|---|
| 18.2.3 | *Undersøgelse af teknisk overensstemmelse*<br><br>Informationssystemer undersøges regelmæssigt for, om de er i overensstemmelse se med organisationens informationssikkerhedspolitikker og -standarder. | Vi har inspiceret, at procedurer for regelmæssig kontrol af systemers overholdelse af sikkerhedsstandarder er implementerede. | Ingen afvigelser konstateret. |