Uafhængig Revisors ISAE 3402 – erklæring

Med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet i relation til leverance af serviceydelser omfattende drift og hosting i perioden 1. maj 2021 til 30. april 2022

Conecto A/S

CVR Nr.: 32 55 09 91

Indholdsfortegnelse

Symbol

- ● Vores gennemgang har ikke ført til bemærkninger.
- ● Der er konstateret svagheder i kontrollerne.
- ● Der er fundet kritiske svagheder eller mangler.

1. Ledelsens Udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Conecto A/S' (herefter "Conecto") leverance af serviceydelser omfattende drift og hosting, 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.

Conecto bekræfter, at:

a) Den medfølgende beskrivelse, afsnit 3, giver en retvisende beskrivelse af leverance af serviceydelser omfattende drift og hosting og de tilhørende kontroller i perioden 1. maj 2021 til 30. april 2022. Kriterierne anvendt for at give 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 sikring af fortrolighed, integritet og tilgængelighed af systemer og data.
   - relevante kontrolmål og kontroller udformet til at nå disse mål.
   - kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen.
   - andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for leverance af serviceydelser.

ii. Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden 1. maj 2021 til 30. april 2022.

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

a) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og fungerede effektivt i perioden 1. maj 2021 til 30. april 2022. Kriterierne anvendt for at give 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 1. maj 2021 til 30. april 2022.

Gladsaxe, 5 juli 2022

Conecto A/S

Tobias Nawrocki

Adm. Direktør

2. Uafhængig Revisors Erklæring om Beskrivelsen af Kontroller, deres Udformning og Funktionalitet

Uafhængig revisors ISAE 3402-erklæring vedrørende informationssikkerhed og foranstaltninger i henhold Conecto A/S' serviceydelser omfattende drift og hosting

Til: Conecto A/S' kunder og deres revisorer

Omfang

Vi har fået til opgave at afgive erklæring om Conecto A/S' (herefter Conecto) beskrivelse i afsnit 3, som beskriver de udførte it-kontroller i relation til leverance af serviceydelser omfattende drift og hosting i perioden 1. maj 2021 til 30. april 2022, og om udformningen og funktionaliteten af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Conectos ansvar

Conecto er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelse er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at opnå de anførte kontrolmål.

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i FSR – danske revisorers retningslinjer for revisors etiske adfærd (Etiske regler for revisorer), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

Grant Thornton er underlagt international standard om kvalitetsstyring, ISQC 1, og anvender og opretholder således et omfattende kvalitetsstyringssystem, herunder dokumenterede politikker og procedurer vedrørende overholdelse af etiske krav, faglige standarder og krav ifølge lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Conectos beskrivelse samt 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.

Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet og fungerer effektivt.

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 samt 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 høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i afsnit 3.

Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

2. Uafhængig Revisors Erklæring om Beskrivelsen af Kontroller, deres Udformning og Funktionalitet

Begrænsninger i kontroller hos Conecto

Conectos beskrivelse 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 vigtigt efter deres særlige forhold. Endvidere vil kontroller hos Conecto som følge af deres art muligvis ikke forhindre eller opdage 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 Conectos system beskrivelse i afsnit 3. Det vores opfattelse, at:

a) at beskrivelsen af kontroller, således som de var udformet og implementeret i perioden 1. maj 2021 til 30. april 2022 i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i perioden 1. maj 2021 til 30. april 2022.

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 perioden 1. maj 2021 til 30. april 2022

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultater af disse test fremgår på i afsnit 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller på i afsnit 4 er udelukkende tiltænkt de kunder, der har anvendt Conectos leverance af serviceydelser på drift og hosting området 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, 5 juli 2022

Grant Thornton
Statsautoriserede revisionspartnerselskab
CVR-nr: 34 20 99 36

Martin Bomholtz
Statsautoriseret revisor

Andreas Moos
Director, Head of IT Audit & Advisory
CISA | CISM

3. Beskrivelse af Generelle IT-kontroller

1.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Conectos kunder og disses revisorer i overensstemmelse med kravene i den danske revisorstandard ISAE 3402 for erklæringsopgaver om kontroller hos serviceleverandøren. Beskrivelsen omfatter informationer om system- og kontrolmiljøet, der er etableret ifm. Conectos leverance af serviceydelser på drift og hosting området.

Systembeskrivelsen indeholder beskrivelser af de anvendte procedurer til sikring af en betryggende afvikling af systemer. Formålet er at give tilstrækkelige informationer til, at drifts og hosting-kunders revisorer selvstændigt kan vurdere afdækningen af risici for kontrolsvagheder i kontrolmiljøet i det omfang, det kan medføre en risiko for væsentlige fejl i drifts og hosting-kunders it-drift.

1.2 Beskrivelse af ydelser der er omfattet af erklæringen

Denne ISAE 3402 erklæring omfatter de hosting og driftsydelser, som Conecto leverer, hvor disse er tilpasset flere forskellige typer af kunder. Betingelserne for de enkelte kunder er angivet i kontrakter, hvor der tages udgangspunkt i standardkontrakter som kan indeholde individuelle tilretninger og optioner. Følgende områder dækker over de kerneydelser, som Conecto tilbyder til deres driftskunder:

Drift af infrastruktur

Conecto er certificerede specialister inden for Citrix portefølje og tilbyder at implementere og drifte en afgrænset del af it-infrastrukturen for kunden. Conectos service inkluderer at opstille en Citrix-baseret infrastruktur som bliver tilpasset ud fra kundens eksisterende infrastruktur og forretningsmæssige behov. Conecto varetager overvågning og proaktiv vedligeholdelse. I Conectos skræddersyede løsninger til kunderne tilbydes der metodik service, der sikrer at kunden har de optimale indstillinger på alle Citrix komponenter. Produktfamilierne Citrix Delivery Center, Citrix Cloud Center og Citrix Online Service sigter mod at gøre databehandling nemmere og mere sikker ved at software leveres som en tjeneste. På denne måde kan man anvende softwaren på mange forskellige typer enheder, når man har en dataforbindelse til rådighed. Citrix Delivery Center, der består af XenDesktop, XenApp, XenServer og NetScaler, virtualiserer servere, brugergrænseflader og programmer. Softwaren centraliseres i datacenteret og leveres til brugerne som en tjeneste.

Conecto tilbyder CTA-ydelser typisk fire gange årligt, hvilke indeholder forbedringsforslag til kundens infrastruktur, som dermed sikrer at de drift-ydelser Conecto tilbyder, følger med udviklingen inden for området.

Conecto består af en bred vifte af kompetencer inden for infrastruktur af IT, hvilket betyder at de certificerede specialister altid kan omstille sig efter kunden behov, til at varetage større dele af kundens drift af IT, hvis nødvendigt. Implementeringen af kundens it-infrastruktur foregår, hvis muligt fysisk, hvor konsulenten har mulighed for at få kundens inputs undervejs i implementeringsprocessen. Conectos driftsydelser foregår derimod remote, hvor ServiceDesk står til rådighed for kunden inden for almindelig arbejdstid. Incident management er forankret i Conectos ServiceDesk, hvor det er muligt at åbne kontakt igennem den tilhørende kundeportal, mail eller via Conectos callcenter. I ServiceDesk bliver alle incidents registreret og prioriteret i henhold til de gældende retningslinjer. Det er ligeledes muligt at eskalere incidents videre til relevante personer eller afdelinger, hvis medarbejderne i ServiceDesken ikke kan løse den pågældende incident. Afrapportering til kunder sker kun der, hvor dette er inkluderet i aftalen med kunden. Omfanget vil være nærmere beskrevet i kundens driftshåndbog.

Beredskabsaftale

Conecto tilbyder kunder 9/5 og 24/7 beredskabsaftaler, inden for den del af infrastrukturen, hvor Conecto har sin specialist viden (core citrix, citrix networking, imprivata mm.). I 24/7 beredskabsaftalen samarbejder Conecto med et eksternt call-center som varetager opkald uden for normal arbejdstid. Conecto responderer på hændelser hele døgnet og call-centret er i besiddelse

3. Beskrivelse af Generelle IT-kontroller

af informationer relaterende til hvilke konsulenter der skal kontaktes i tilfælde af hændelser hos en given beredskabs- eller driftskunde. Hvis kunden har købt en 9/5 beredskabsaftale, og uheldet sker uden for tidsrummet, kan Conecto stadig tilbyde sin assistance mod et ekstra omkostningsgebyr.

1.3 Intern organisering af it-sikkerhed

Ledelsen i Conecto, som er den øverst ansvarlige for it-sikkerhed, sørger for, at der er etableret procedurer og systemer, der understøtter overholdelsen af den til enhver tid gældende it-sikkerhedspolitik. It-sikkerhedsgruppen beskriver de overordnede målsætninger, og den driftsansvarlige i form af Customer Succes Manageren, er ansvarlig for udarbejdelse og implementering af relevante kontroller til efterlevelse af it-sikkerhedspolitikken. Sikkerhedsniveauet skal være målbart og kontrollabelt, hvor dette overhovedet er muligt, og være udtryk for best practice inden for de enkelte kontrolaktiviteter på de serviceområder, som tilbydes kunderne. It-sikkerhedsgruppen består pt. af følgende medlemmer:

- Lars Forup Frederiksen – Customer Success manager
- Bo Nielsen – Project Manager
- Christian Fenneberg – Chief Technical Officer

Gruppen mødes i forbindelse med den årlige revision for at fastlægge og følge op på målsætninger i relation til it-sikkerheden. Når It-sikkerhedsgruppen har udarbejdet risikoanalysen, bliver rapporten præsenteret for den administrerende direktør, og det er hermed direktørens ansvar at godkende risikoanalysen og sikre at den årlige revision bliver gennemført, med udgangspunkt i risikovurderingen. Hvis risikoanalysen ikke bliver godkendt, skal it-sikkerhedsgruppe sammen med den administrerende direktør, opstille en proces der sikrer et lavere trusselsniveau mod Conectos it-sikkerhed, samt en godkendt risikoanalyse.

1.4 It-sikkerhedspolitik

Conecto it-sikkerhedspolitik skaber rammerne for systematisk operationel ledelse af informationssikkerhed (ISMS), der udmøntes i etableringen af fastsatte retningslinjer for håndtering af Conecto it-sikkerhed. Dermed etableres et grundlag for det daglige arbejde med it-sikkerhed i Conecto. Ansvarsplacering, retningslinjer, risikohåndtering og it-beredskabsplaner er således emner, der reguleres under ISMS.

Conectos it-sikkerhed er baseret på:

- Almindeligt accepterede metoder og politikker for informationssikkerhed.
- Alle relevante regler, lovkrav, retningslinjer, vejledninger og kontrakter inden for driftsafdelingen (operations) i Conecto

En ledelsesgodkendt it-sikkerhedspolitik er udarbejdet med udgangspunkt i en it-risikoanalyse, og kommunikeret ud til relevante medarbejdere i virksomheden.

Anvendte procedurer og kontroller

Conecto afdækker relevante it-risici på driftsydelserne. Dette varetages gennem en løbende trussels- og risikovurdering hos Conecto i forbindelse med en årlig revurdering af risikoanalysen. Resultatet af den årlige gennemgang forlægges for ledelsen. Conecto stiller endvidere en række informationer til rådighed for drift-kundernes revisorer, til brug for deres vurdering af Conecto som driftsleverandør.

Tidspunkt for udførsel af kontrollen

It-sikkerhedspolitikken revurderes mindst en gang årligt forinden udførelse af it-revisionen og udarbejdelse af erklæring.

Hvem udfører kontrollen

Den årlige gennemgang udføres af den driftsansvarlige sammen med de øvrige medlemmer af IT sikkerhedsgruppen.

3. Beskrivelse af Generelle IT-kontroller

Kontrol dokumentation

Der er versionsstyring af it-sikkerhedspolitikken

1.5 Risikostyring

Risikostyring gennemføres i Conecto på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering, der primært er orienteret mod interne systemer. Inputs til denne vurdering indhentes på tværs af hele organisationen. Risiko- og trusselsvurderingen er bygget op over test vedrørende den fysiske sikkerhed samt test af interne systemer og danner grundlag for beredskabsplanen. Direktøren for Conecto er øverste ansvarlige for, at der bliver udført risikoanalyser, og den driftsansvarlige er som en del af it-sikkerhedsgruppen ansvarlig for udførelsen. Den samlede beredskabsplan bliver opdateret i forbindelse med den årlige revision. Chefen for den enkelte afdeling er ansvarlig for, at de risikoanalyser, der kræver ændringer i beredskabsplanen, bliver foretaget.

Risikovurderingen står beskrevet i Conectos it-sikkerhedspolitik, hvor hver enkelt trussel er tildelt et risikotal der er summen af en vurdering af sandsynlighed og konsekvens. De etablerede trusler mod Conectos serviceydelser inden for drift og hosting er ved seneste risikoanalyse identificeret ud fra sandsynlighed og konsekvens.

1.6 Medarbejdere og uddannelse

Medarbejderne i Conecto skriver i ansættelseskontrakten under på overholdelse af gældende ordens- og arbejdsbestemmelser samt IT-sikkerhedspolitik, som er vedlagt i ansættelseskontrakten. Medarbejdere underskriver ved ansættelse også en fortrolighedserklæring, som omhandler hvordan medarbejderen behandler kundernes data. Enkelte medarbejdere er sikkerhedsgodkendte, der hvor kravet er aftalt med kunden.

Medarbejderne modtager uddannelse, træning og oplysning om informationssikkerhed fra nærmeste leder, således niveauet er passende og relevant i forhold til medarbejderens arbejdsopgaver, ansvarsområde og evner. Ligeledes inkluderer dette aktuelle informationer om kendte trusler, samt om hvem der skal kontaktes for yderligere råd angående informationssikkerhed. Den enkelte medarbejder har ansvar for at overholde it-sikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver, samt for at rapportere eventuelle brud på it-sikkerheden eller mistanke herom til it-sikkerhedsfunktionen.

Som ansat i Conecto har man løbende samtaler med nærmeste leder om uddannelse og udvikling i organisationen hvor der årligt bliver lagt en plan for hvilke certificeringer der er relevante for den enkelte medarbejder for at kunne varetage de arbejdsopgaver, som er forventet af den ansatte.

Ved ansættelse af ny medarbejder tildeler ServiceDesk de relevante rettigheder efter opfordring fra den nærmeste leder. Efter afskedigelse af medarbejder sikrer ServiceDesk at medarbejderens adgang bliver slettet i Conectos systemer. ServiceDesk kontakter også medarbejderens kunder, så log-in og adgang hos kunden bliver slettet, med henblik på at mindske sandsynlighed for svindel efter opsigelse af en medarbejder.

1.7 Adgangsstyring

Udgangspunktet for tildeling af rettigheder og adgang til systemer og informationer er, at alt er låst ned og at der kun gives adgang, hvor der er et forretningsmæssigt behov.

Den ansvarlige for et system og eller informationerne beslutter hvem, der skal have adgang til systemet og/eller informationerne. Conecto ServiceDesk tildeler herefter rettighederne ud fra disse beslutninger.

Bærbare pc'er beskyttes med adgangskode og skærmlås samt opdaterede antivirusprogrammer og lokale firewalls.

Styring af adgangskoder følger Best Practice - minimum 8 karakterer, kombination af store/små bogstaver samt tal.

Conectos øvrige mobile enheder (mobiltelefoner og evt. tablets) beskyttes med en 4 cifret pinkode samt mulighed for sletning (remote-wipe) af enhederne.

3. Beskrivelse af Generelle IT-kontroller

Conectos fysiske lokaler er sikret med adgangssystem og alarmsystem. Den ansvarlige for lokationen beslutter hvem, der skal have adgang til hvad.

1.7.1 Fysisk sikring og miljøsikring

Der er etableret fysisk adgangskontrol, således kun autoriserede personer, der har et arbejdsrelateret behov for adgang, kan opnå adgang med adgangschip og nøgle. Adgangsrettighederne til at sikre områder gennemgås og ajourføres i en kontrolliste, hvor udleveret adgangschip og nøgle underskrives af medarbejderen ved ansættelse. Hvis den ansatte mister nøgler eller adgangskort, er der indarbejdet procedure for skift af nøgler og adgangschip.

Ved besøg af gæster, der skal have adgang til bygningen, skal disse være under konstant opsyn af værten. Medarbejderen bliver gjort opmærksom på disse retningslinjer ved ansættelse i form af udleveret personalehåndbog.

Conecto anvender Sentia som datacenter, hvor der henvises til Sentia's særskilte ISAE 3402 erklæring for den fysiske sikring af servere og data i datacenteret.

1.8 Informationer og aktiver

Conectos informationer findes på it-aktiver som eksempelvis pc'er, servere, tablets, smartphones, usb-nøgler, cloud-lagre og lignende. Sikkerhedspolitikken kræver, at Conectos informationer er beskyttet i tilfælde af tab, tyveri, kopiering mv.

Kryptering af virksomhedens informationer understøttes af en begrænsning af hvilke personer, der får rettigheder til at læse, rette eller slette informationer. Her henvises til afsnittet adgangsstyring.

Medarbejdere i Conecto må som udgangspunkt ikke opbevare firmarelaterede data i et cloud-lager, som Dropbox, med mindre dette er stillet til rådighed af Conecto, eller godkendt af Conectos ledelse til firmabrug. Hvis der opstår et akut behov for at opbevare firmarelaterede data i et ikke-godkendt cloud-lager, er det medarbejderens ansvar at sørge for, at data er krypterede.

Conectos it-aktiver (software, informationer eller fysisk udstyr) registreres således den enkelte medarbejders it-aktiver kan dokumenteres.

Nye it-anskaffelser skal overholde Conectos retningslinjer, herunder krav om beskyttelse med antivirus mv. og evt. om kryptering. Er der tale om en helt ny anskaffelse, som en ny type pc'er eller et nyt økonomisystem vurderes det, om der sker ændringer i trusselsbilledet og om der i så fald skal stilles specifikke krav.

1.9 Klassifikation

Arbejdet med at afgøre hvem der må tilgå hvad samt hvordan informationer skal behandles, kan lettes og strømlines med indførelsen af en klassifikation, som kort fortæller, hvad man må med informationerne.

I Conecto er alle informationer som udgangspunkt klassificeret som "intern", hvilke betyder at informationer må ses/tilgås af alle i Conecto og hos specifikke kunder/samarbejdspartnere. Den enkelte medarbejder skal dermed ikke klassificere en mail eller et dokument hvis det er internt, da denne klassifikation er standart i Conecto.

Hvis informationerne derimod kun må ses/tilgås af en mindre gruppe med et konkret forretningsmæssigt formål, skal mailen eller dokumentet klassificeres som værende følsomt. Informationer klassificeret som følsomt, bør mærkes med deres klassifikation på forsiden af dokumenter hvad enten de er på papir eller i elektronisk form.

1.10 Driftssikkerhed

Tilgængeligheden af systemer og data sikres gennem en fortsat drift i tilfælde af mulige forstyrrelser. Dette sikres bl.a. gennem kontroller, der er imødegående, afbødende eller overvågende. Kontrollerne ligger inden for fysiske kontroller, procedurekontroller, tekniske kontroller og lovmæssigt styrede kontroller. Disse kontroller dækker bl.a. over følgende: autentifikation, antivirus, firewall, incident management, låse, brandalarmer, driftscenteret (er skalsikret med brudsikkert glas), UPS, nødstrømsanlæg, Inergen-brandslukning, monitorering, backup og beredskabsplaner. Disse kontroller udføres af it-sikkerhedsgruppen.

3. Beskrivelse af Generelle IT-kontroller

Der er indarbejdet adgangsstyring for håndtering og godkendelse af såvel interne som kunders brugerid'er. Der er fastlagte passwordpolitikker for autentifikation og tofaktorautentifikation, som er udmøntet i standarder.

Conecto foretager patchning af operativsystemet efter leverandørens anbefalinger (Windows). Fuldt patchede systemer gælder også der, hvor det specifikt er angivet i kontrakter og driftshåndbøger.

Kundens data sikres, ved at struktureringen af netværket opbygges af VLAN's, således de enkelte kunder kun kan tilgå deres eget netværk.

Der er udarbejdet formelle forretningsgange for ændringsstyring. Formålet med dette er, at risikoen for kompromittering af virksomhedens og kundernes informationer minimeres. Introduktionen af nye systemer og større ændringer til de eksisterende systemer følger en formel proces med dokumentation, specifikation og styret implementering. Ændringsstyring i Conecto følger retningslinjer og procedurer for ændringsstyring.

Effektiv monitorering af processer giver vigtige oplysninger til både proaktivt og reaktivt at kunne undgå events, der ellers ville have påvirket overholdelsen af kundernes SLA. Målet er at minimere den tid, det tager at genetablere normal drift. For at imødegå dette arbejder Conecto med forebyggende monitorering og dertilhørende korrigerende handlinger. Ved denne metode sker der ingen eller minimal påvirkning af kundens SLA.

Der, hvor det ikke er muligt at forudse events, benyttes detekterende monitorering med dertilhørende korrigerende handlinger. Denne metode gør det muligt at reagere i henhold til kundernes SLA.

Logning af aktiviteter er slået til i Conectos systemer, hvor det giver mening, og hvor der er persondata, logges adgang og forsøg på adgang til de enkelte informationer også. For at opretholde driftssikkerheden foretager ServiceDesk patching, back-up, sårbarhedsanalyse og overvågning over egne og kunders IT-systemer.

1.11 Kommunikationssikkerhed

Conecto anvender Citrix og brugernes webadgang til internettet er tilgængeligt gennem Citrix Workspace. Conecto udøver kontrol vha. sikkerhedsprodukter fra Citrix og Cisco. Adgang til usikre hjemmesider blokeres og filer, der downloades, bliver scannet for virus og andet malware af ServiceDesk.

Conectos interne netværk er beskyttet med en firewall, der regulerer og logger trafikken mellem Conectos interne net og Conectos tele-/internetleverandør, så kun tilladt trafik passerer igennem. Derudover er firewallen sat op med et separat netværk (DMZ) med adgang fra internettet til specifikke services og med meget begrænset adgang til Conecto interne netværk. I DMZ findes Conecto webserver og andre eksterne services.

Conectos interne netværk er delt i to netværk, et servernet og et klientnet, som firewallen kontrollerer trafikken imellem. Firewallregler er så vidt muligt konfigureret i henhold til PCI-compliance, hvilket betyder at der kun åbnes for de nødvendige services og kun mellem relevante netværkssegmenter, samt at der er defineret regler for både indgående og udgående netværkstrafik.

Brugernes webadgang til internettet scannes i en cloud/proxy-løsning for at tilsikre at der ikke tilgås usikre hjemmesider. Adgang til usikre hjemmesider blokeres og filer, der downloades, bliver scannet for virus og andet malware.

Alle indgående e-mails, der modtages i Conectos mailsystem, bliver scannet for usikre links til eksterne hjemmesider og for om det er en potentiel phishing-mail. Derudover scannes vedhæftede filer for virus og andet malware. Der er etableret en standartadvarsel for eksterne mails, for at forhindre at medarbejderne kan tage fejl af hvilke mails der er sendt fra internt i organisationen og hvilke der ikke er.

Al ekstern adgang til Conectos netværk og systemer sker via krypterede (VPN) forbindelser. Conectos website og webservices benytter https-kryptering baseret på Transport Layer Security (TLS), ligesom mailserveren også håndterer TLS.

3. Beskrivelse af Generelle IT-kontroller

Adgang til andre servere/services og Conectos interne netværk sker via klientkryptering beskyttet af 2-faktor autentifikation.

Overførsel af, eller adgang til, Conectos informationer til/fra eksterne samarbejdspartnere eller myndigheder må kun ske efter aftale med disse, baseret på informationernes fortrolighed, herunder om evt. brug af kryptering.

Pc'er og mobile enheder, der kobler sig på virksomhedens netværk og systemer eksternt fra, skal overholde virksomhedens retningslinjer. Dette er kun tilladt for virksomhedens udstyr og gælder også medarbejdernes egne pc'er og mobile enheder (Bring Your Own Device, BYOD).

1.12 Kryptering

Der anvendes kryptering på al ekstern kommunikation til og fra datacentreret. Der anvendes enten Ipsec, VPN eller SSL.

1.13 Styring af informationssikkerhedsbrud

Hvis en medarbejder opdager trusler mod, eller brud på, informationssikkerheden, eller får mistanke om det, skal vedkommende straks underrette Conecto ServiceDesk om dette.

ServiceDesk som er ansvarlig for den daglige styring af Conecto informationssikkerhed vurderer de rapporterede sikkerhedshændelser hurtigst muligt efter at de er anmeldt. Såfremt eksterne parter berøres af sikkerhedshændelser hos Conecto, er den daglige ledelse ansvarlig for eventuel kommunikation over for berørte parter.

1.14 Styring af sikkerhedshændelser

Hvis der konstateres en sikkerhedshændelse, adviseres de berørte kunder så hurtigt som muligt, og samtidigt tages der skridt til at sikre data og systemer. Efterfølgende udarbejdes en rapport til kunden, for så vidt muligt at sikre at hændelsen ikke kan optræde igen.

Er der tale om en intern medarbejder, der har overtrådt, eller forsøgt at overtræde, sikkerhedsreglerne uforsætligt, gives vedkommende ved første tilfælde en mundtlig advarsel og ved andet tilfælde en skriftlig advarsel. Sker det tredje gang, tages der skridt til afskedigelse af den pågældende medarbejder.

Hvis medarbejdere forsætligt overtræder, eller forsøger at overtræde, sikkerhedsreglerne, tages der straks

skridt til afskedigelse, og i særligt grove tilfælde vil der være tale om bortvisning. Alle sikkerhedshændelser rapporteres til it-sikkerhedsgruppen og ledelsen.

1.15 Informationssikkerhedsaspekter ved ned-, beredskabs- og reetableringsstyring

Katastrofer søges undgået gennem en veltilrettelagt fysisk sikring og overvågning af bygninger, tekniske installationer og it-udstyr. Omfanget af disse foranstaltninger besluttes ud fra en afvejning af risici imod sikringsomkostninger og udmøntes i SLA'er.

Der er etableret en task force i Conecto der iværksættes når/hvis beredskabsplaner skal aktiveres ved eventuelle nedbrud eller trusler. Denne taskforce er under ledelse af it-sikkerhedsgruppen og er defineret i Conectos beredskabsplaner.

Udover den etablerede taskforce indeholder beredskabsplanen fire scenarier som er opstillet af it-sikkerhedsgruppen med udgangspunkt i seneste risikovurdering.

Til at imødekomme risici foretages der mindst en gang årligt test af Conecto beredskabsplaner med dertilhørende dokumentation. Testplanen er bygget op over test vedrørende den fysiske sikkerhed samt test af kunderelaterede systemer og ajourføres efter behov.

3. Beskrivelse af Generelle IT-kontroller

1.16 Mitigerende kontroller hos kunden

Forudsætninger vedrørende kundernes ansvar er beskrevet i individuelle kontrakter og driftshåndbøger. Kunden er ansvarlig for egne data. Det betyder, at kunden er ansvarlig for de ændringer, der måtte foretages i data, når der er logget på systemet med individuelle brugernavne og adgangskoder. Ved tredjepartsadgang bestilt af kunden er det kunden, som har ansvaret for opfølgning af kontrollen. Der er enkelte kunder, som ifølge deres kontrakt har mulighed for test af backup. Kunderne er selv ansvarlige for at initiere test af backupplan.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

4.1 Formål og omfang

Den følgende oversigt er udformet for at skabe en forståelse for effektiviteten af de kontroller, som Conecto 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 nået i perioden d. 1. maj 2021 til 30. april 2022.

Vi har således ikke nødvendigvis testet alle de kontroller, som Conecto har nævnt i sin beskrivelse i afsnit 3. Kontroller udført hos Conecto A/Ss kunder er herudover ikke omfattet af vores erklæring, idet kundernes egne revisorer må foretage denne gennemgang og vurdering.

4.2 Udførte testaktiviteter

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

Vi har udført vores tests af kontroller hos Conecto ud fra nedenstående metoder:

Metode	Overordnet beskrivelse
Forespørgelse	Interview af udvalgte medarbejdere angående kontroller
Observation	Observation af hvordan kontroller udførelse (Design)
Inspektion	Gennemgang af politikker, procedurer og dokumentation af kontrollernes udførelse (Implementering)
Test af kontrol	Gennemførelse af kontrolhandlinger, som vi selv har udført eller som har observeret gennemført af ansvarlige medarbejdere (Udførelse)

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

4. Risikovurdering og -håndtering

Kontrolmål:
At sikre, at virksomheden løbende identificerer, analyserer og vurderer risici relateret til organisationen.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
4.1	Kontroller er etableret, som tilvejebringer rimelig sikkerhed for, at processer for risikovurdering er implementeret, og at risikovurderingen foretages minimum årligt.	Vi har inspiceret, at risikovurderingen er opdateret og godkendt. Vi har inspiceret, at Conectos risikoeksponering styres baseret på risikoscoren, som beregnes ud fra sandsynlighed og konsekvens.	Ingen væsentlige afvigelser konstateret.
4.2	Kontroller er etableret, som sikre at der foretages en regelmæssig vurdering og gennemgang af risici og disse behandles i ledelsesteamet, hvor ledelsen vurderer, om nye risici er opstået og derfor kræver yderligere analyse og håndtering.	Vi har inspiceret, at risikovurderingen opdateres minimum årligt.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

5. Informationssikkerhedspolitikker

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
5.1	Der er udarbejdet en it-sikkerhedspolitik som er godkendt af Conectos ledelse. Conecto sikrer dette ved at kommunikere revisioner og opdateringer i hele organisationen via bevidsthed træningsprogrammer, e-mails såvel som på afdelingen og personalemøder.	Vi har inspiceret at Conecto har en informationssikkerhedspolitik. Vi har inspiceret dokumentation for at denne er godkendt i perioden.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

6. Organisering af informationssikkerhed

Kontrolmål:
At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
6.1	Alt ansvar for informationssikkerhed skal defineres og fordeles. Modstridende pligter og ansvarsområder er adskilt for at reducere mulighederne for uautoriseret eller utilsigtet ændring eller misbrug af organisationens aktiver.	Vi har inspiceret, at ansvar og roller for informationssikkerhed er defineret og allokeret til kvalificerede medarbejdere. Vi har inspiceret beskrivelse af roller og ansvarsområder i informationsikkerhedsorganisationen. Vi har inspiceret dokumentation for adskillelse af funktioner.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

6. Organisering af informationssikkerhed

Kontrolmål:
At sikre fjernarbejdspladser og brugen af mobilt udstyr.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
6.2	Informationssikkerhedspolitikken inkluderer kontroller til fjernadgang og der er implementeret sikkerhedsforanstaltninger for at sikre fjernadgang.	Vi har inspiceret politikken og kontroller for styring af mobilenheder. Vi har inspiceret dokumentation for at tekniske sikkerhedsforanstaltninger i forbindelse med fjernarbejde er implementeret.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

7. Medarbejdersikkerhed

Kontrolmål:
At sikre, at medarbejder og kontrahenter forstår deres ansvar og er egnede til de roller, de er tiltænkt.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
7.1	Conecto har etableret formelle procedurer for ansættelse af nye medarbejdere. Personer, der tilbydes en stilling i Conecto, vil blive genstand for en baggrundskontrol før de begynder ansættelse. Medarbejderne bekræfter ved underskrift på deres ansættelseskontrakt, at de er forpligtet til at være bekendt med indholdet af kontrakten og er underlagt tavshedspligt.	Vi har observeret, at der er en formel procedure for ansættelse af nye medarbejdere. Vi har stikprøvevis inspiceret at der foretages screening af medarbejdere inden ansættelse. Vi har inspiceret en standard ansættelseskontrakt samt standard tjekliste i forbindelse med ansættelse. Vi har stikprøvevis inspiceret ansættelseskontrakter og tjeklister i forbindelse med ansættelse medarbejdere.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

7. Medarbejdersikkerhed

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
7.2	Conectos ledelse stiller krav til at medarbejdere og kontrahenter overholder krav om informationssikkerhed. Conecto udfører awareness-træning samt afdelings og personalemøder til at sikre, at medarbejdere er bekendte med politikker og procedurer. Der er implementeret sanktioner for overtrædelse af informationssikkerhedspolitikken.	Vi har forespurgt omkring ledelsens ansvar for at formidle politikker og procedurer. Vi har inspiceret dokumentation for afholdelse af awareness træning, samt inspiceret at alle relevante medarbejdere har deltaget i awareness træning. Vi har forespurgt til retningslinjer for sanktionering af medarbejdere i forbindelse med brud på interne retningslinjer vedrørende informationssikkerhed.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
7.3	Informationssikkerhedsansvar og –forpligtelser er gældende efter ansættelsens ophør.	Vi har stikprøvevis inspiceret at der er udfyldt en standard meddelelse til fratrådte i forbindelse med fratrædelse.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

8. Styring af aktiver

Kontrolmål:
At identificere organisationens aktiver og definere passende ansvarsområder og beskyttelse heraf.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
8.1	Conecto har registreret væsentlige it-aktiver i en række systemer og defineret ejerskab for kategorier af aktiver. Retningslinjer for accepteret brug af al informationsrelateret aktiver findes og er tilgængelige for relevante medarbejdere.	Vi har inspiceret fortegnelsen over aktiver. Vi har inspiceret fortegnelsen over aktiver og inspiceret at hvert aktiv har en udpeget ejer. Vi har inspiceret politik for accepteret brug af aktiver indeholder beskrivelse af hvordan aktiver må bruges.	Ingen væsentlige afvigelser konstateret.

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
8.2	Aktiver er klassificeret og mærket, hvor det er fundet relevant. Der er implementeret procedurer, som sikrer at aktiver håndteres iht. informationssikkerhedspolitikken.	Vi har forespurgt til procedure for mærkning af information. Vi har inspiceret procedurer til mærkning af information.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

8. Styring af aktiver

Kontrolmål:
At forhindre uautoriseret offentliggørelse, ændring fjernelse eller destruktion af information lagret på medier.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
8.3	Der er implementeret kontroller til at sikre håndtering af bærbare medier.	Vi har inspiceret proceduren for styring af bærbare medier. Vi har inspiceret proceduren for bortskaffelse af medier. Vi har inspiceret, at bærbare medier er blevet sikkert destrueret.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

9. Adgangsstyring

Kontrolmål:
At begrænse adgangen til information og informationsbehandlingsfaciliteter.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
9.1	Der er en politik og procedure for tildeling, ændring og tilbagekaldelse af adgangsrettigheder for medarbejdere.	Vi har inspiceret politikken og proceduren for tildeling, ændring og tilbagekaldelse af adgangsrettigheder. Vi har inspiceret politikken for adgangsstyring.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

9. Adgangsstyring

Kontrolmål:
At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
9.2	Der findes en formel forretningsprocedure for tildeling og tilbagekaldelse af brugeradgange. Tildeling og anvendelse af udvidede adgangsrettigheder er begrænset og overvåget. Interne brugers adgangsrettigheder gennemgås regelmæssigt i henhold til en formaliseret forretningsprocedure.	Vi har inspiceret procedurer for tildeling og tilbagekaldelse af brugeradgange. Vi har stikprøvevis inspiceret tildeling og tilbagekaldelse af brugeradgange er foretaget i overensstemmelse med proceduren. Vi har forespurgt om håndtering af privilegerede adgangsrettigheder. Vi har inspiceret dokumentation for gennemgang af brugeradgangsrettigheder.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

9. Adgangsstyring

Kontrolmål:
At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
9.3	Adgangskoder er personlige og holdes hemmelige.	Vi har inspiceret skriftlige krav til kvaliteten af adgangskoder.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At forhindre uautoriseret adgang til systemer og applikationer.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
9.4	Adgang til operativsystemer og netværk er beskyttet af adgangskoder.	Vi har forespurgt til begrænsning af adgang til information og sikker log-on procedurer.	Ingen væsentlige afvigelser konstateret.
	Der er etableret kontroller, der giver rimelige forsikring om, at administratoradgang er begrænset til personer med et arbejdsrelateret behov for adgang.	Vi har inspiceret at administratoradgang er begrænset til personer med et arbejdsrelateret behov for adgang.	

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

10. Kryptografi

Kontrolmål:
At sikre passende og effektiv brug af kryptering for at beskytte fortroligheden, autenticitet og/eller integritet.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
10.1	Der er i informationssikkerhedspolitikken sat krav om, at al kommunikation på åbne, offentlige netværk skal være krypteret. Adgang til systemer fra andre lokationer er krypteret via VPN. Skift af krypteringsnøgler sker efter en fastsat procedure.	Vi har inspiceret, at der anvendes kryptering på transmission over internettet. Vi har inspiceret at der benyttes VPN forbindelser til adgang til systemer fra andre lokationer. Vi har inspiceret, at der er procedure for skift af krypteringsnøgler.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

11. Fysisk sikring og miljøsikring

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
11.1	Alle informationsrelaterede aktiver er beskyttet mod uautoriseret adgang i datacentre og kontorer med adgangssystemer, overvågning og alarmer. Kontroller giver rimelig sikkerhed for at adgange tildeles i henhold til forretnings- og arbejdsrelaterede behov. Alle informationsrelaterede aktiver er beskyttet mod brand, vand og varme.	Vi har observeret de fysiske sikkerhedsparametre for Conectos lokation. Vi har inspiceret, at datacenterleverandørs ISAE 3402 erklæring dækker kontroller, der vedrører adgangskontroller, adgangssystemer, overvågning og alarmering. Vi har inspiceret, at datacenterleverandørens ISAE 3402 erklæring dækker kontroller, der vedrører understøttende forsyninger og vedligeholdelse af disse, samt at der er implementeret sikkerhedsforanstaltninger til sikring mod og opdagelse af ild, vand og varme. Vi har inspiceret leverandørers erklæringer for outsourcet drift og vedligehold af faciliteter i erklæringsperioden.	Datacenterleverandørs ISAE 3402 erklæring er kun dækkende indtil ultimo december 2021. Ingen yderligere væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

11. Fysisk sikring og miljøsikring

Kontrolmål:
At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
11.2	Alle informationsrelaterede aktiver er beskyttet mod strømafbrydelse via UPS og nødstrømsystemer. Kabler til elektronisk kommunikation og elektricitet forsyningen er beskyttet mod manipulation. Medarbejdere er underlagt krav om clean desk og der er implementeret skærmlås. Data der bærer informationsrelaterede aktiver, bortskaffes på en sikker måde.	Vi har inspiceret, at datacenterleverandørens ISAE 3402 erklæring dækker kontroller, der vedrører UPS og nødstrømssystemer og at kabler er beskyttet mod manipulation. Vi har inspiceret vejledning til clean desk og bruger udstyr uden for opsyn, herunder at der er skærmlås. Vi har inspiceret dokumentation for sikker bortskaffelse af medier.	Datacenterleverandørs ISAE 3402 erklæring er kun dækkende indtil ultimo december 2021. Ingen yderligere væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

12. Driftssikkerhed

Kontrolmål:
At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.1	Der er dokumenterede driftsprocedurer for forretningskritiske systemer og disse er tilgængelige for medarbejdere med arbejdsrelaterede behov. Funktionsadskillelse er implementeret i driftsprocedurer. Der er etableret kontroller, der giver rimelige forsikring om, at Conecto har etableret en formel proces for ændringsstyring, der sikrer test og godkendelse af relevante ændringer.	Vi har inspiceret dokumenterede driftsprocedurer er tilgængelige for medarbejdere. Vi har inspiceret, at der er funktionsadskillelse i driftsprocedurer. Vi har inspiceret procedurer for ændringsstyring. Vi har stikprøvevis inspiceret at proceduren for ændringsstyring har været fulgt.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

12. Driftssikkerhed

Kontrolmål: **At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware**			
Nr.	***Kontrol Aktivitet***	***Revisors udførte test***	***Resultat af revisors test***
12.2	Der er etableret kontroller, der sikrer identifikation, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har inspiceret dokumentation for kontroller mod malware. Vi har inspiceret de implementerede løsninger til opdagelse af malware.	Ingen væsentlige afvigelser konstateret.

Kontrolmål: **At beskytte mod tab af data**			
Nr.	***Kontrol Aktivitet***	***Revisors udførte test***	***Resultat af revisors test***
12.3	Der er etableret kontroller, der giver rimelige forsikring om, at processerne vedrørende backup og gendannelse af data er tilfredsstillende.	Vi har inspiceret, at der er dokumenterede procedurer for backup, og at der er foretaget faste backup job. Vi har inspiceret, at backup foretages af relevante systemer og at backup udføres i henhold til fastsat skema. Vi har inspiceret, at der følges op på mislykkede backup jobs.	Ingen yderligere væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

12. Driftssikkerhed

Kontrolmål: **At registrere hændelser og tilvejebringe bevis.**			
Nr.	***Kontrol Aktivitet***	***Revisors udførte test***	***Resultat af revisors test***
12.4	Der er implementeret systemer til overvågning af server- og netværksdrift.	Vi har inspiceret, at events udløser et event i overvågningssystemet, og at medarbejderne håndterer begivenhederne ud fra vigtighed og effekt. Vi har inspiceret de anvendte foranstaltninger til beskyttelse af log information. Vi har inspiceret at effektiviteten af overvågningssystemet jævnligt kontrolleres. Vi har inspiceret, at synkronisering af tid er implementeret.	Ingen væsentlige afvigelser konstateret.

Kontrolmål: **At sikre integriteten af driftssystemer**			
Nr.	***Kontrol Aktivitet***	***Revisors udførte test***	***Resultat af revisors test***
12.5	Der er etableret kontroller, der giver rimelig sikkerhed for, at driftsplatformen er patchet i henhold til retningslinjer.	Vi har inspiceret procedurer til styring af softwareinstallation på driftssystemer. Vi har inspiceret, at mislykkede eller manglende patches og opdateringer registreres og håndteres.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

12. Driftssikkerhed

Kontrolmål:
At forhindre, at tekniske sårbarheder udnyttes.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.6	Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer. Sårbarheder evalueres og der implementeres foranstaltninger for at håndtere disse.	Vi har inspiceret dokumentation for implementerede foranstaltninger til identifikation af tekniske sårbarheder.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At forhindre indvirkningen af audit aktiviteter på driftssystemer

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
12.7	Der gennemføres løbende revisioner af interne aktiviteter samt leverandørers overholdelse af kontrakter.	Vi har inspiceret, at Conecto har modtaget og evalueret erklæringer fra væsentlige leverandører.	Datacenterleverandørs ISAE 3402 erklæring er kun dækkende indtil ultimo december 2021. Ingen yderligere væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

13. Kommunikationssikkerhed

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
13.1	Der er etableret kontroller til sikring af netværket.	Vi har inspiceret, at netværket administreres, dokumenteres og at denne dokumentation opdateres ved ændringer. Vi har inspiceret, at der er passende procedurer til administration af netværksudstyr. Vi har inspiceret, at netværket er passende segmenteret og er sikres via firewalls. Vi har inspiceret, at produktionsmiljøet er designet og implementeret som et redundant opsætning.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At opretholde informationssikkerhed ved overførelse internt i organisation til en ekstern entitet.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
13.2	Der er etableret politikker og procedurer, samt kontroller til beskyttelse af informationer ved overførsel.	Vi har inspiceret politikker og procedurer for informationsoverførsel. Vi har stikprøvevis inspiceret, at indgåede aftaler indeholder beskrivelse af aspekter vedrørende informationsoverførsel. Vi har inspiceret dokumentation for at emails kan leveres krypteret.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

15. Leverandørforhold

Kontrolmål:
At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
15.1	Risici forbundet med eksterne forretningspartnere identificeres og sikkerhed i tredjepartsaftaler styres.	Vi har inspiceret informationssikkerhedspolitikken for leverandørforhold. Vi har inspiceret at informationssikkerhed er inkorporeret i leverandøraftaler.	Ingen væsentlige afvigelser konstateret.

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
15.2	Leverandører overvåges regelmæssigt, herunder styring ifm. ændringer af leverandørydelser.	Vi har inspiceret informationssikkerhedspolitikken for leverandørforhold. Vi har inspiceret, at Conecto har modtaget og evalueret erklæringer fra væsentlige leverandører.	Datacenterleverandørs ISAE 3402 erklæring er kun dækkende indtil ultimo december 2021. Ingen yderligere væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

16. Styring af informationssikkerhedsbrud

Kontrolmål:
At sikre ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og –svagheder.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
16.1	Sikkerhedshændelser rapporteres til ledelsen så snart som muligt, og de styres på en ensartet og effektiv måde.	Vi har inspiceret procedurerne for håndtering af hændelser inklusiv rapportering af sikkerhedshændelser. Vi har inspiceret at hændelser bliver rapporteret, og at roller og ansvarsområder er defineret. Vi har stikprøvevis inspiceret, at hændelser er blevet registreret og håndteret i henhold til procedurerne.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Kontrolmål:
At informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
17.1	Der er etableret kontroller som sikrer informationssikkerhedskontinuiteten er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.	Vi har inspiceret at beredskabsplanen er opdateret og godkendt i perioden. Vi har inspiceret at der er foretaget test af beredskabsplanen i perioden.	Ingen væsentlige afvigelser konstateret.

Kontrolmål:
At sikre tilgængelighed af informationsbehandlingsfaciliteter.

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
17.2	Der er etableret kontroller til at sikre tilgængelighed af informationsbehandlingsfaciliteter.	Vi har forespurgt om tilgængelighed af informationsbehandlingsfaciliteter. Vi har inspiceret dokumentation for at informationsbehandlingsfaciliteter er redundante.	Ingen væsentlige afvigelser konstateret.

4. Kontrolmål, Kontrolaktivitet, Test og Resultat heraf

18. Overensstemmelse

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
18.1	Conecto har etableret procedurer og kontroller til at undgå brud på lov-, myndigheds- og kontraktkrav relateret til informationssikkerheds og andre sikkerhedskrav. Kontroller er etableret hvor det er relevant for at sikre privatliv og beskyttelse af personhenførbare informationer samt krav til kryptering.	Vi har forespurgt omkring kontroller til at identificere lov- og kontraktmæssige krav. Vi har inspiceret at implementerede kontroller omkring beskyttelse af privatliv og personhenførbare informationer.	Ingen væsentlige afvigelser konstateret.

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

Nr.	*Kontrol Aktivitet*	*Revisors udførte test*	*Resultat af revisors test*
18.2	Conecto har etableret kontroller til at sikre at informationssikkerhed er implementeret og håndteret i overensstemmelse med virksomhedens politikker og procedurer.	Vi har inspiceret implementerede kontroller til at sikre overholdelse af krav i virksomhedens politikker og standarder.	Ingen væsentlige afvigelser konstateret.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Tobias Rune Nawrocki
Underskriver 1
På vegne af: Conecto A/S
Serienummer: 4aa0f707-bc22-48e2-a100-7b2d5ef7e0f6
IP: 217.63.xxx.xxx
2022-07-06 13:19:35 UTC
MitID

Andreas Moos
Underskriver 2
Serienummer: PID:9208-2002-2-411646217865
IP: 62.243.xxx.xxx
2022-07-06 13:33:08 UTC
NEM ID

Martin Bomholtz
Underskriver 3
Serienummer: PID:9208-2002-2-013768766685
IP: 62.243.xxx.xxx
2022-07-06 13:45:15 UTC
NEM ID

Penneo dokumentnøgle: 02UHZ-M5IH0-H8GAJ-LW26J-BUPE0-JS2NW