cBrain A/S

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller for perioden fra 1. januar 2023 til 31. december 2023 i relation til cBrains F2- og M4-ydelser

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Indhold

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

1 Serviceleverandørens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for de kunder, der har anvendt cBrains ydelser relateret til F2- og M4-løsningerne, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har udført ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

cBrain anvender Sentia som serviceunderleverandør for it-drift. Beskrivelsen i sektion 3 medtager kun kontrolmål og kontrolaktiviteter hos cBrain og medtager således ikke kontrolmål og underliggende kontrolaktiviteter hos Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørens kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af cBrains kontroller, er passende designet og er operationelt effektive sammen med relaterede kontroller hos cBrain. Beskrivelsen omfatter ikke kontrolaktiviteter udført af kunder.

cBrain bekræfter, at:

(a) Den medfølgende beskrivelse, i sektion 3, giver en retvisende beskrivelse af generelle it-kontroller i relation til cBrains F2- og M4-ydelser, der har behandlet kunders transaktioner i perioden fra 1. januar 2023 til 31. december 2023. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   (i) redegør for, hvordan generelle it-kontroller i relation til cBrains F2- og M4-ydelser var udformet og implementeret, herunder redegør for:

      - de typer af ydelser, der er leveret
      - processer i både it- og manuelle systemer
      - de tilhørende regnskabsregistreringer, underliggende information og specifikke konti, der blev anvendt til at igangsætte, registrere, behandle og rapportere transaktioner, herunder korrektionen af ukorrekt information, og hvordan informationen er overført til de rapporter, der er udarbejdet til kunder
      - hvordan systemet behandlede andre betydelige begivenheder og forhold
      - processen, der blev anvendt til at udarbejde rapporter til kunder
      - ydelser udført af underleverandører, hvis relevant, herunder om de er medtaget efter helhedsmetoden eller udeladt efter partielmetoden
      - relevante kontrolmål og kontroller designet til at nå disse mål
      - kontroller, som vi med henvisning til systemets design har forudsat ville være implementeret af brugervirksomhederne, 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 (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante

   (ii) indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden fra 1. januar 2023 til 31. december 2023

   (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.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

(b) de kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og var operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023, hvis relevante kontroller hos underleverandører var hensigtsmæssigt designet og operationelt effektive, og kunder har udført de komplementerende kontroller, som forudsættes i designet af cBrains kontroller i perioden fra 1. januar 2023 til 31. december 2023. Kriterierne for denne udtalelse var, at

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

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

(iii) kontrollerne var udført konsistent som designet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i perioden fra 1. januar 2023 til 31. december 2023.

København, den 24. januar 2024
cBrain A/S

Robert Lentz
direktør

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

2 Serviceleverandørs uafhængige revisors erklæring

Uafhængig revisors ISAE 3402-erklæring om sikkerhed om beskrivelse af kontroller, deres design og operationel effektivitet for perioden fra 1. januar 2023 til 31. december 2023 i relation til cBrains F2- og M4-ydelser

Til: cBrain A/S, cBrain A/S' kunder og deres revisor

Omfang

Vi har fået som opgave at afgive erklæring om cBrains beskrivelse i sektion 3 (beskrivelsen) af sine generelle it-kontroller i relation cBrains F2- og M4-ydelser, der har behandlet kunders transaktioner i perioden fra 1. januar 2023 til 31. december 2023, og om design og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen angiver, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan opnås, hvis komplementerende kontroller hos kunderne, der forudsættes i designet af cBrains kontroller, er passende designet og operationelt effektive sammen med relaterede kontroller hos cBrain. Vores handlinger har ikke omfattet kontrolaktiviteter udført af kunderne, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos kunderne.

cBrain anvender Sentia som serviceunderleverandør for it-drift. Beskrivelsen i sektion 3 medtager kun kontrolmål og relaterede kontroller hos cBrain og medtager således ikke kontrolmål og relaterede kontroller hos Sentia. Beskrivelsen angiver også, at visse kontrolmål, der er specificeret i beskrivelsen, kun kan nås, hvis underleverandørers kontroller, der forudsættes i designet af cBrains kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos cBrain. Vores handlinger har ikke omfattet kontrolaktiviteter udført af Sentia, og vi har ikke vurderet egnetheden af design eller den operationelle effektivitet af kontrolaktiviteter hos underleverandører.

cBrains ansvar

cBrain er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter; for at anføre kontrolmålene; identifikation af de risici der påvirker opnåelsen af kontrolmålene; udvælgelsen af de kriterier der er præsenteret i ledelsens udtalelse; samt for designet, implementeringen og operationel effektive kontroller for at nå de anførte kontrolmål.

Vores 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.

EY Godkendt Revisionspartnerselskab anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Vores ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om cBrains beskrivelse samt om design og den operationelle effektivitet 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 høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og operationelt effektive.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og operationel effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes design og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt designet eller ikke er operationelt effektive.

Vores handlinger har omfattet test af den operationelle effektivitet 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 sektion 1.

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

cBrains 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 en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet 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 sektion 1. Det er vores opfattelse,

(a) at beskrivelsen af, hvordan generelle it-kontroller i relation til cBrains F2- og M4-ydelser, således som det var designet og implementeret i perioden fra 1. januar 2023 til 31. december 2023, i alle væsentlige henseender er retvisende,

(b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden fra 1. januar 2023 til 31. december 2023, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis de relaterede kontroller var hensigtsmæssigt designet i perioden fra 1. januar 2023 til 31. december 2023, og hvis kontroller hos underleverandører og komplementerende kontroller hos kunder var hensigtsmæssigt designet og implementeret i perioden fra 1. januar 2023 til 31. december 2023, som forudsat i designet af cBrains kontroller, og

(c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har været operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023, hvis kontroller hos underleverandører har været operationelt effektive, og hvis de komplementerende kontroller hos kunder, der forudsættes i designet af cBrains kontroller, har været operationelt effektive i perioden fra 1. januar 2023 til 31. december 2023.

Beskrivelse af test af kontroller

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

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i sektion 4 er udelukkende tiltænkt kunder, der har anvendt generelle it-kontroller i relation til cBrains F2- og M4-ydelser, 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 24. januar 2024
EY Godkendt Revisionspartnerselskab
CVR-nr. 30 70 02 28

Jesper Due Sørensen
Partner

Johanna Kansonen-Valtersdorf
statsaut. revisor
mne48476

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

3 Beskrivelse af generelle it-kontroller vedrørende ydelser relateret til F2 og M4 og implementeret af cBrain

3.1 Indledning

cBrain er leverandør af F2- og M4-løsningerne med tilhørende ydelser til cBrains kunder.

Løsningerne understøtter vores kunder i en lang række forskellige digitale forretningsprocesser, som involverer medarbejdere, medlemmer, borgere, myndigheder og virksomheder. Løsningerne er implementeret i organisationer i både privat sektor og i offentlig sektor. De digitale forretningsprocesser kan fx være sags- og dokumenthåndtering, medlemshåndtering, mødebooking, ledelsesbetjening, tilskudsadministration, afgørelser, godkendelser og meget mere. Kunder er placeret i Danmark og internationalt.

Når en organisation er gået i drift, er cBrains ydelser karakteriseret ved, at cBrain er;

- leverandør af drift
- leverandør af support
- leverandør af ad hoc-opgaver.

cBrain er leverandør af drift

Kunden har en driftsaftale, og løsningen er placeret i cBrains driftsmiljø, som fysisk er placeret hos Sentia. I dette tilfælde er det cBrains ansvar at sikre, at driften udføres i henhold til aftalte Service Level Agreements og i henhold til de sikkerhedsbestemmelser, som er indgået.

cBrain er leverandør af supportydelser

Kunden har en aftale om programmelvedligeholdelse, og i den forbindelse gives der adgang til supportydelser. I forbindelse med udførelse af supportydelser, har cBrain adgang til kundens systemer og data. Adgangen til data og dermed behandlingen af data sker udelukkende med henblik på at afhjælpe kundens problem eller spørgsmål i relation til det programmel, som indgår under aftalen om programmelvedligeholdelse. Er der tale om fejl i programmel, afhjælpes problemet med rettelser til programmel.

cBrain er leverandør af ad hoc-opgaver

Kunden har en aftale om, at der kan ske leverance af ad hoc-opgaver. Yderligere leverancer er reguleret af leverancekontrakten og betegnes som Ændringsønsker eller Change Request. Følgende opgaver er typiske ad hoc-opgaver:

- opgradering
- installation af patch
- serverskift
- uddannelse
- konvertering
- aflevering til Rigsarkivet.

3.2 Sikkerhedsmæssige foranstaltninger

Der er etableret et veldokumenteret kontrolapparat for understøttelse af sikkerhed for databehandling i de tre overordnede ydelser for henholdsvis drift, support og ad hoc-opgaver.

cBrain har tilrettelagt it-sikkerheden med udgangspunkt i ISO 27001. Processer i tilknytning til F2-produktet og medarbejdere ansat i Danmark er ISO 27001-certificeret. Væsentlige dele af ISO-certificeringen overlapper med de procedurer, som også er i anvendelse i relation til M4-løsningen.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Som led i cBrains Information Security Management udføres hvert kvartal kontroller af it-sikkerhedsforhold, fx restore-test af F2- og M4-kundesystemer samt kontrol af antivirus og server-patchning. cBrain afholder hvert kvartal it-management sikkerhedsreview-møde, hvor risici og behov for ændringer gennemgås, herunder specifikt i forhold til de senest registrerede sikkerhedsrelaterede hændelser (security related incidents). cBrain gennemfører endvidere årligt intern it-sikkerhedsaudit, hvor politikker, Standard Operating Procedures og kontroller gennemgås.

cBrain anvender Sentia som samarbejdspartner i forbindelse med levering af driftsydelser.

Sentia er en full-service hosting-virksomhed. Selskabet leverer professionelle it-services til offentlige og private virksomheder. Ydelserne omfatter virtuelle løsninger, co-location (fysiske rackskabe), driftsløsninger og outsourcing, backup (inklusive remote backup), storage, professionelle internetforbindelser, IP-trafik og sikrede omgivelser. Sentia driver datacentre i Danmark, der er redundant forbundet og forbundet med Danmarks største teleknudepunkter.

I relation til samarbejdet med cBrain leverer Sentia kun de fysiske rammer for driften, mens cBrain ejer og administrerer hardware og software inklusive basis-software, databaser m.m. Kun cBrains medarbejdere har adgang til cBrains servere på Sentias lokationer i Danmark. Kunders data inklusive backup er placeret i Danmark. Sentias administrative personale har ikke adgang til at forbinde til cBrains servere. Af supporthensyn for maksimal oppetid og evt. fejlfinding har Sentia dog administrative rettigheder til firewall i Taastrup.

Gennem ejerskabet af servere m.m., som både er placeret hos Sentia og i cBrains kontorlokaler, kan cBrain sikre, at personer fra sikre/usikre tredjelande eller internationale organisationer ikke har adgang til at behandle data, f.eks. via support (herunder "se-adgang") eller udvikling.

It-sikkerheden hos Sentia efterprøves ved, at de hvert år får udarbejdet ISAE 3000- og 3402-erklæringer. Deres ISAE-erklæringer gennemgås og godkendes efterfølgende i cBrain. Det bemærkes, at denne ISAE-rapport ikke inkluderer de ydelser, som Sentia leverer.

De generelle aftaler omkring behandling af data og instrukser er anført i databehandleraftalen.

Incident management proces

cBrains medarbejdere har pligt til straks at indberette formodede sikkerhedshændelser eller svagheder. Informationssikkerhedshændelser logges centralt, vurderes og tildeles derefter til den relevante sikkerhedsejer til information og løsning. cBrains procedure for håndtering af sikkerhedsbrud, inkl. underretning af påvirkede kunder, om:

a. Karakteren af bruddet på sikkerheden

b. Sandsynlige konsekvenser af brud på sikkerheden

c. Foranstaltninger, der er truffet eller foreslået for at håndtere brud på sikkerheden.

På Management Review-møder i cBrain gennemgås hvert kvartal hændelser og det bestemmes, hvilke fremtidige ændringer i IT-sikkerheden, der skal implementeres. Opfølgningshandlinger registreres i sikkerhedsloggen og spores indtil de lukkes.

Medarbejdere

Medarbejdere er underlagt fortrolighedserklæringer og der er etableret processer for on-boarding, off-boarding og job-change, som sikrer, at adgangsforhold m.m. stemmer overens med ansættelsesforhold. En lang række af cBrains medarbejdere er sikkerhedsgodkendte, for at kunne arbejde med kunder i den offentlige sektor. Der udføres løbende opmærksomhedstiltag (awareness training) med henblik på at sikre, at medarbejdere kontinuerligt bliver opdateret på sikkerhedstiltag og processer.

Udvikling af programmel udføres af medarbejdere ansat af cBrain i Danmark og de støttesystemer, som anvendes til programmelvedligeholdelse og supporthenvendelser er ejet af cBrain og bliver driftet og vedligeholdt af cBrain-medarbejdere i Danmark.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Logning

cBrain bruger en række overvågningsværktøjer til at sikre, at systemerne er operationelle, og for at blive advaret, hvis noget er galt. Alle sikkerhedsrelaterede handlinger på cBrains kritiske servere logges i tilfælde af, at en hændelse kræver yderligere undersøgelse. Active Directory (AD) ændringer overvåges ved hjælp af en kombination af gruppepolitikker og logovervågningsværktøjer. cBrains softwareprodukter M4 og F2 logger brugeroperationer og logs kan tilgås af administratorer.

Netværkssikkerhed

I cBrain bruges flere metoder til styring af netværk, for at beskytte information i systemer og applikationer. cBrains netværk er beskyttet af firewalls. Al trafik til firewalls administreres og logges. Trådløs adgang er adskilt i to separate netværk – et produktionsnetværk, hvor alle virksomhedens arbejdsstationer er forbundet samt et gæstenetværk. Virtuelle netværk er etableret for at sikre adskillelse af adgang på tværs af miljøer.

Logisk adgang

cBrain har en password-politik, som styres via Active Directory. Når cBrains medarbejdere tilgår kundesystemer er det kundens password-politik, der efterleves. Der logges brugerhandlinger i cBrains systemer og disse logs kan tilgås af administratorer. cBrains F2-system muliggør granuleret rettighedsstyring af adgang til data. cBrains bærbare devices er krypterede, og der er krav om, at følsomme data i transit også skal være krypterede.

Der foretages regelmæssige kontroller af adgangsrettigheder til servere og systemer i cBrain. Der arbejdes med standarder for sikkerhed omkring adgangsstyring til data og niveauer for beskyttelse udført i samarbejde med kunden. Der er kontrolforanstaltning og rapportering i de tilfælde, hvor kunden afviger fra den anbefalede tilgang.

Fysisk adgang

Adgang til cBrains danske hovedkvarter er kun mulig ved brug af adgangschip samt kode uden for arbejdstiden, eller i arbejdstiden ved anmodning om adgang gennem receptionen. cBrains danske kontor har alarm til registrering af indtrængen. Interne servere og fortrolige oplysninger opbevares i aflåselige rum med adgang begrænset til få navngivne personer. Servere, der hoster kundedata, hostes i professionelle eksterne datacentre med passende fysiske sikkerhedskontroller. Ingen kundedata må hostes på cBrain-kontorer.

På eksternt datacenter i Danmark - med cBrains kundedata - er der kun fysisk adgang for datacenters driftspersonale samt relevante underleverandører med personlige akkrediteringer. Det er et Tier 2 tilsvarende center. Der er 24 timers 100 % kapacitet datacenterdrift backup via dieselgenerator. Det testes ved faste frekvenser for at sikre, at disse fungerer korrekt. Datacenteret er klassificeret som en kritisk del af den danske infrastruktur, bl.a. på grund af internettransit, og er dermed sikret daglige leveringer af diesel 30 dage i træk. Der er redundant køleanlæg med 2 individuelle kølekompressorer, som giver fri køling ved lave udetemperaturer. Der er system til beskyttelse mod vandlækage og røg- og branddetektorer samt Argonite brandslukningssystemer. Der er 24x7 kameraovervågning med teknikere på stedet, samt overvågning af køle- og elsystemer.

Change Management proces

Sikkerhedskrav vurderes under designfasen for en ny funktion og testes før implementering. Al softwarekode skal vedligeholdes i cBrains officielle kodelager og placeres under versionskontrol.

Planlægningen af, hvilke funktioner der skal implementeres, styres gennem et product board, som gennemgår og godkender ændringer af softwaren. Der er en kontrolprocedure for hasteændringer, som er godkendt gennem en defineret godkendelsesproces. Alle ændringer bliver gennemgået og testet uafhængigt af udvikleren og underskrevet af QA, før de accepteres i en produktionsudgivelse. Alle ændringer i cBrains F2 software foretages først i udviklingsmiljø, dernæst i kundernes testsystemer og sluttelig i kundernes produktionssystemer. Der foretages test i hvert af miljøerne, så fejl så vidt muligt opfanges, inden ændringerne lægges i kundernes produktionssystemer.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Der er Standard Operating Procedures (SOP) for en lang række aktiviteter, herunder for håndtering af personhenførbare data i forbindelse med supportrapporteringer. Der er indført protokoller for, hvad der er tilladt, hvordan og hvornår der slettes data fra supportsystemer.

Backup-proces

Der tages natlig backup af servere og databaser. Kvartalsvis foretages der restoretests af kunde M4- og F2-systemer til sikring af, at backups er anvendelige og at genskabelsesrutiner er indøvede.

Beredskabsstyring

cBrain A/S hoster udvalgte kunders M4- og F2-systemer. Forpligtelserne for cBrain over for kunderne er styret af kontrakterne mellem cBrain og hver enkelt kunde. Baseret på disse kontrakter har cBrain en forpligtelse til at genetablere både data og tjenester i tilfælde af en katastrofe.

cBrain har fastslået, at informationssikkerhedskravene for gendannelse af service er de samme som for igangværende driftstjenester, og derfor gælder de samme sikkerhedsordninger. I dette tilfælde betyder det, at kun kvalificeret og autoriseret personale i Operations er autoriseret til at få adgang til hosting-miljøet og gendanne tjenesten.

cBrain afprøver årligt sine beredskabsplaner for genetablering af M4- og F2-services.

3.3 Risikovurdering

cBrain gennemfører mindst en gang årligt en risikovurdering. Vurderingen tager udgangspunkt i KOMBITs standard for risikovurdering. Selve vurderingen tager udgangspunkt i en række potentielle hændelser, hvoraf risikoen for tab af fortrolighed, tab af integritet og tab af tilgængelighed indgår. For hver af disse er der foretaget en vurdering af risikoen for, at hændelsen indtræffer, og hvilken konsekvens denne måtte have (Konsekvens for den registrerede, Omdømme, Økonomisk osv.).

cBrains ledelse afholder kvartalsvis Management Review møder, som bl.a. behandler compliance i forhold til ISO27001. Management Review møder er et krav under ISO27001.

3.4 Kontrolforanstaltninger

Der er indført en lang række kontrolforanstaltninger, som til dels er anbefalet i forhold til ISAE 3000- og 3402-aktiviteter, målrettet beskyttelse af persondata og i forhold til ISO 27001-aktiviteter. Kontrolforanstaltninger bliver løbende justeret og revideret i forhold til risikovurderinger og ændringer i markedsforhold generelt.

Der henvises i øvrigt til afsnit 4, hvor de konkrete kontrolaktiviteter er beskrevet.

3.5 Komplementerende kontroller hos kunderne

Kunderne har følgende forpligtelser:

- At sikre sig, at kundens brugere er ajourførte.
- At sikre sig, at adgangsforhold lever op til markedsstandarder for sikker adgang, herunder egne brugers og cBrains adgang til kunders data.
- cBrain kan med forudgående aftale med kunden opsætte logning i systemerne. Det er dermed kundens eget ansvar at tage stilling til de opsatte logningskrav i brugergrænsefladen i M4 og F2. Kunderne er også selv ansvarlige for, at logs gennemgås regelmæssigt. Det er kun medlemsadministratorrollen hos kunderne, som har adgang til loggen.
- Kunder på F2 og M4 skal selv tildele medarbejdere en rolle, der giver forskellige niveauer af adgange til løsningerne. Det er kundens eget ansvar at sikre, at disse rettigheder kun gives til relevante ansatte og det niveau af adgang, den enkelte medarbejder bør have.
- Hver kunde har adgang til et testmiljø og et produktionsmiljø, som er selvstændige installationer til den enkelte kunde. Det er kundernes eget ansvar at sikre, at testdata på testmiljøet ikke indeholder data på virkelige personer.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

4 Tests udført af EY

4.1 Formål og omfang

Vores arbejde blev gennemført i overensstemmelse med ISAE 3402, "*Erklæringer med sikkerhed om kontroller hos en serviceleverandør*", og de yderligere krav, der er gældende i Danmark.

Vores test af kontrollers design, implementering og operationelle effektivitet har omfattet de kontrolmål og tilknyttede kontroller, der er udvalgt af ledelsen, og som fremgår af sektion 4. Eventuelle andre kontrolmål, tilknyttede kontroller og komplentære kontroller hos kunden eller kontroller, som er beskrevet i sektion 3, men ikke fremgår af sektion 4, er ikke omfattet af vores test.

Test af operationel effektivitet har omfattet de kontroller, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået i perioden fra 1. januar 2023 til 31. december 2023.

4.2 Udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og funktion er beskrevet nedenfor:

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. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. På de tekniske platforme, databaser og netværkskomponenter har vi testet den specifikke systemopsætning for at påse, om kontroller er designet og effektive i perioden fra 1. januar 2023 til 31. december 2023.
Forespørgsler	Forespørgsel af passende personale hos cBrain. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

4.3 Kontrolmål, kontrolaktivitet, test og resultat heraf

Kontrolmål: 5.1 Retningslinjer for styring af informationssikkerhed At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
5.1.1	***It-sikkerhedspolitik*** Ledelsen godkender en skriftlig informationssikkerhedspolitik, som offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.	Inspiceret, at informationssikkerhedspolitikken er godkendt af ledelsen og kommunikeret til medarbejdere og relevante eksterne parter. Inspiceret, at politikken er gjort tilgængelig for medarbejderne på intranettet.	Ingen afvigelser konstateret.
5.1.2	***Evaluering af it-sikkerhedspolitikken*** Informationssikkerhedspolitikken evalueres med planlagte mellemrum, eller i tilfælde af væsentlige ændringer, for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	Inspiceret, at informationssikkerhedspolitikken er opdateret. Vi har inspiceret informationssikkerhedspolitikken for at sikre, at den er fyldestgørende.	Ingen afvigelser konstateret.

Kontrolmål: 6.1 Intern organisering At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i virksomheden.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
6.1.1	***Roller og ansvarsområder for informationssikkerhed*** Alt ansvar for informationssikkerhed er klart defineret.	Inspiceret dokumentation, som viser, at ansvaret for informationssikkerheden er klart defineret i politikker.	Ingen afvigelser konstateret.
6.1.2	***Funktionsadskillelse*** Modstridende ansvarsområder er adskilt for at reducere mulighederne for uautoriseret eller utilsigtet ændring eller misbrug af organisationens aktiver.	Inspiceret, at områder med nødvendig funktionsadskillelse er defineret og gennemgået. Inspiceret, for en stikprøve af ændringer, at funktionsadskillelse opretholdes i ændringshåndteringsprocessen. Inspiceret, for en stikprøve af brugere, at funktionsadskillelse opretholdes i adgangshåndteringsprocessen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 6.2 Mobilt udstyr og fjernarbejdspladser At sikre fjernarbejdspladser og brugen af mobilt udstyr.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
6.2.1	***Mobilt udstyr og kommunikation*** Der er etableret en formel politik, og passende sikkerhedsforanstaltninger er iværksat for at beskytte mod de risici, som anvendelse af mobilt udstyr og kommunikationsudstyr indebærer.	Inspiceret politikken for implementering af sikkerhedsforanstaltninger til mobilt udstyr og kommunikationsudstyr. Inspiceret, at der er implementeret en installationsprocedure for mobilt udstyr med henblik på, at opsætningen af mobilt udstyr sikrer datas fortrolighed.	Ingen afvigelser konstateret.
6.2.2	***Fjernarbejdspladser*** Der er udarbejdet og implementeret en politik og operationelle planer og procedurer for fjernarbejde via mobilarbejdspladser.	Inspiceret politikkerne for fjernarbejde via mobilarbejdspladser.	Ingen afvigelser konstateret.

Kontrolmål: 7.1 Inden ansættelse At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
7.1.2	***Ansættelsesvilkår og -betingelser*** Som led i den kontraktlige forpligtelse underskriver medarbejdere, kontrahenter og eksterne konsulenter betingelserne i ansættelseskontrakten, der angiver deres og cBrains ansvar for informationssikkerhed.	Stikprøvevist inspiceret på nyansatte og ekstern konsulent i erklæringsperioden, at ansættelseskontrakten inkluderer en specificering af ansvar i forhold til informationssikkerhed samt indeholder krav om tavshedspligten. Inspiceret ansættelseskontraktlige skabeloner for medarbejdere, kontrahenter og eksterne konsulenter, og konstateret, at disse inkluderer en specificering af ansvar i forhold til informationssikkerhed samt indeholder krav om tavshedspligten.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 7.2 Under ansættelse At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
7.2.1	***Ledelsens ansvar*** Ledelsen kræver, at medarbejdere, kontrahenter og eksterne konsulenter opretholder sikkerheden i overensstemmelse med virksomhedens fastlagte politikker og procedurer.	Inspiceret beskrivelsen af ledelsens krav til medarbejdere, kontrahenter og eksterne konsulenter. Stikprøvevist inspiceret at kommunikation fra ledelsen til medarbejdere, hvori det påpeges, at sikkerhedspolitikken skal overholdes.	Ingen afvigelser konstateret.
7.2.2	***Bevidsthed om, uddannelse og træning i informationssikkerhed*** cBrains medarbejdere og, hvor det er relevant, kontrahenter og eksterne konsulenter bevidstgøres om sikkerhed og holdes regelmæssigt ajour med cBrains politikker og procedurer, i det omfang det er relevant for deres jobfunktion.	Inspiceret procedurer for sikring af tilstrækkelig awareness-træning og regelmæssig opdatering af organisationens politikker og procedurer. Inspiceret, at cBrain har udført aktiviteter, der understøtter sikkerhedsbevidstheden blandt medarbejdere. Inspiceret, at ansatte eksterne konsulenter i erklæringsperioden indgår som en del af awareness-træningen.	Ingen afvigelser konstateret.
7.2.3	***Sanktioner*** Der er etableret en formel sanktionsprocedure, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.	Inspiceret, at der findes en formel sanktionsprocedure for medarbejdere, der bryder cBrains retningslinjer for informationssikkerhed. Forespurgt, om der har været registreret medarbejdere, som tilsigtet eller utilsigtet har overtrådt sine loyalitetsforpligtelser i erklæringsperioden.	cBrain har oplyst, at der ikke har været registreret nogen medarbejdere, som tilsigtet eller utilsigtet har overtrådt sine loyalitetsforpligtelser i erklæringsperioden. Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 7.3 Ansættelsesforholdets ophør eller ændring At sikre, at ophør eller ændring af medarbejderes, kontrahenters og eksterne brugeres ansættelse finder sted på en betryggende måde.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
7.3.1	***Inddragelse af adgangsrettigheder*** Medarbejderes, kontrahenters og eksterne konsulenters adgangsrettigheder til informationer og informationsbehandlingsudstyr inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Inspiceret proceduren vedrørende ophør af ansættelse for at kontrollere, at ansvaret for at ændre eller bringe et ansættelsesforhold til ophør er placeret. Stikprøvevist inspiceret fratrådte medarbejdere og ekstern konsulent med henblik på at konstatere, om medarbejderne havde fået inddraget deres adgangsrettigheder.	Ingen afvigelser konstateret.

Kontrolmål: 9.1 Forretningsmæssige krav til adgangsstyring At begrænse adgangen til information og informationsbehandlingsfaciliteter.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
9.1.1	***Politik for adgangsstyring*** Der er udarbejdet en politik for adgangsstyring, som dokumenteres og evalueres på grundlag af forretnings- og sikkerhedsmæssige krav til adgang.	Inspiceret politikken for adgangsstyring med henblik på at konstatere, om den var opdateret og godkendt.	Ingen afvigelser konstateret.
9.1.2	***Politik for adgang til netværk og netværkstjenester*** Brugere får kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Inspiceret, at proceduren for tildeling af adgang til tjenester til brugere sker ud fra et arbejdsrelateret behov. Stikprøvevist inspiceret brugere med henblik på at konstatere, at de kun havde adgang til godkendte tjenester, der var tildelt ud fra et arbejdsrelateret behov.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 9.2 Administration af brugeradgang At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
9.2.1	***Brugerregistrering og -afmelding*** Der er implementeret en formel procedure for registrering og afmelding af brugere.	Inspiceret proceduren for registrering og afmelding af brugere. Stikprøvevist inspiceret brugere, der henholdsvis til- og fratrådte i erklæringsperioden med henblik på at konstatere, om procedurerne for brugeroprettelse og -nedlæggelse er fulgt.	Ingen afvigelser konstateret.
9.2.3	***Styring af privilegerede adgangsrettigheder*** Tildeling og brug af privilegerede adgangsrettigheder er begrænset og kontrolleret.	Inspiceret retningslinjer for begrænsning og styring af tildeling og anvendelse af privilegier. Stikprøvevist inspiceret, at privilegerede brugere havde et arbejdsbetinget behov for adgang.	Ingen afvigelser konstateret.
9.2.4	***Administration af brugeradgangskoder (password)*** Tildeling af adgangskoder styres ved hjælp af en formel administrationsproces.	Inspiceret proceduren vedrørende styring af tildeling af adgangskoder.	Ingen afvigelser konstateret.
9.2.5	***Gennemgang af brugeradgangsrettigheder*** Ledelsen evaluerer administrative brugers adgangsrettigheder årligt ved hjælp af en formel proces.	Inspiceret proceduren for årlig evaluering af administrative adgangsrettigheder. Inspiceret, at der er udført årlig evaluering af administrative brugergennemgange for AD-administratorrettigheder samt cBrains interne F2-administratorer.	Ingen afvigelser konstateret.
9.2.6	***Inddragelse eller justering af adgangsrettigheder*** Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Inspiceret proceduren for ansættelsesophør og fjernelse og rettelse af adgangsrettigheder. Stikprøvevist inspiceret fratrådte brugere, med henblik på at konstatere, om medarbejderne havde fået fjernet deres adgangsrettigheder i relevante systemer.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 9.3 Brugernes ansvar At sikre, at passende forretningsprocedurer er på plads for at mindske risikoen for tab af ægthed, integritet og fortrolighed.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
9.3.1	***Password-politikker*** Det er et krav, at brugere følger cBrains praksis ved anvendelse af hemmelig autentifikationsinformation.	Inspiceret procedure vedrørende definition af kvalitetskrav for adgangskoder. Inspiceret, at den implementerede politik for brug af adgangskoder automatisk påtvinger brugerne til at følge den formelle procedure for adgangskoder.	Ingen afvigelser konstateret.

Kontrolmål: 9.4 Styring af system- og applikationsadgang For at sikre, at der er tilstrækkelig kontrol på plads med hensyn til datakommunikation, som passende sikrer mod risikoen for tab af ægthed, integritet og fortrolighed.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
9.4.2	***Procedurer for sikkert log-on*** Adgang til driftssystemer er styret af en procedure for sikker log-on.	Inspiceret procedure for kontrol af adgang til driftssystemer. Inspiceret procedure vedrørende definition af kvalitetskrav for adgangskoder. Inspiceret, at der anvendes unikke bruger-id og adgangskoder ved log-in.	Ingen afvigelser konstateret.
9.4.5	***Styring af adgang til kildekoder til programmer*** Adgang til kildekoder til programmer er begrænset.	Inspiceret procedurer vedrørende begrænsning af adgang til programmers kildekode. Stikprøvevist inspiceret kildekodefiler med henblik på at konstatere, om adgang hertil var begrænset til medarbejdere, der har et arbejdsbetinget behov for adgang til kildekoden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 11.1 Sikre områder At forebygge uautoriseret fysisk adgang, beskadigelse og forstyrrelser i organisationens informations- og informationsbehandlingsfaciliteter.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
11.1.1	***Fysisk perimetersikring*** cBrain har implementeret fysisk parametersikring for at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.	Inspiceret procedurer vedrørende fysisk sikring af faciliteter og perimetersikkerhed. Inspiceret relevante lokationer og deres indbyggede perimetersikkerhed for at konstatere, hvorvidt der er taget forholdsregler for at forhindre uautoriseret adgang.	Ingen afvigelser konstateret.
11.1.2	***Fysisk adgangskontrol*** Sikre områder er beskyttet med passende adgangskontroller for at sikre, at kun autoriseret personale får adgang.	Inspiceret proceduren for beskyttelse af sikre områder. Observeret flere adgangspunkter med henblik på at konstatere, at der skal anvendes personligt adgangskort for at få adgang til cBrains faciliteter.	Ingen afvigelser konstateret.

Kontrolmål: 12.1 Driftsprocedurer og ansvarsområder At sikre, at der er etableret passende forretningsgange og kontroller i forhold til driften og ændringsstyring, og at der er etableret passende adskillelse af miljøer mellem udvikling, test og drift.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.1.1	***Dokumenterede driftsprocedurer*** Driftsprocedurer er formaliseret og stilles til rådighed for relevante medarbejdere.	Inspiceret, at driftsprocedurer er formaliserede og dokumenterede og er gjort tilgængelige for personalet.	Ingen afvigelser konstateret.
12.1.3	***Kapacitetsstyring*** Anvendelsen af ressourcer styres og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.	Inspiceret procedurer for overvågning og tilpasning af kapacitetskrav for at sikre fremtidige kapacitetskrav. Stikprøvevist inspiceret, at der foretages overvågning af ressourceanvendelsen på netværksområdet.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 12.1 Driftsprocedurer og ansvarsområder At sikre, at der er etableret passende forretningsgange og kontroller i forhold til driften og ændringsstyring, og at der er etableret passende adskillelse af miljøer mellem udvikling, test og drift.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.1.4	***Adskillelse af udviklings-, test- og driftsmiljøer*** Udviklings-, test- og driftsservere er adskilt.	Stikprøvevist inspiceret, at der er en logisk adskillelse mellem udviklings-, test- og driftsmiljøer.	Ingen afvigelser konstateret.

Kontrolmål: 12.2 Beskyttelse mod malware At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.2.1	***Kontroller mod malware*** Der er implementeret kontroller til detektering, forhindring og gendannelse med henblik på at beskytte mod malware, kombineret med passende brugerbevidsthed.	Inspiceret procedurer for forebyggelse og detektering af et udbrud af ondsindet kode og reetablering efter et ondsindet virusangreb. Stikprøvevist inspiceret enheder med henblik på at konstatere, om virusbeskyttelse er installeret, kørende og opdateret.	Ingen afvigelser konstateret.

Kontrolmål: 12.3 Backup At beskytte mod tab af data.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.3.1	***Backup af information*** Der er taget backupkopier af informationer, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backup-politik.	Inspiceret procedurer vedrørende backup af systemer og data. Stikprøvevist inspiceret at backupkopier foretages som beskrevet i procedurerne. Inspiceret overvågningen af daglig backup for at konstatere, hvorvidt succesfulde og fejlede backup-jobs blev bemærket, og hvorvidt der blev fulgt op på fejlede backup-jobs.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 12.4 Logning og overvågning At sikre, at der er etableret passende kontroller til overvågning, registrering og opfølgning på relevante operationelle hændelser.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.4.1	***Hændelseslogning*** Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Inspiceret, at der foreligger krav til omfang og indhold af hændelseslogninger. Inspiceret, at der er opsat auditlogning. Inspiceret, at der udføres regelmæssig gennemgang af logs.	Ingen afvigelser konstateret.
12.4.2	***Beskyttelse af logoplysninger*** Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Inspiceret proceduren for beskyttelse af logningsfaciliteter og logge. Stikprøvevist inspiceret at logningsinformationer fra servere og systemer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	***Administrator- og operatørlog*** Aktiviteter udført af systemadministratorer og -operatører logges.	Inspiceret procedurer for logning af aktiviteter, der udføres af systemadministratorer og -operatører. Stikprøvevist inspiceret logkonfiguration på servere med henblik på at konstatere, om systemadministratorers og -operatørers handlinger logges.	Ingen afvigelser konstateret.
12.4.4	***Tidssynkronisering*** Urene i relevante informationsbehandlingssystemer er synkroniseret med NTP-pools.	Inspiceret proceduren for synkronisering af ure med en aftalt, præcis tidsangivelse. Inspiceret, at der er opsat systemparametre, der sikrer synkronisering med aftalt tidskilde.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 12.5 Sikring af systemfiler At sikre integriteten af driftssystemer.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.5.1	***Softwareinstallation i driftssystemer*** Der er etableret procedurer for styring af softwareinstallationen på driftssystemer.	Inspiceret proceduren for softwareinstallation på driftssystemer. Stikprøvevist inspiceret softwareinstallationer med henblik på at konstatere, om proceduren er fulgt.	Ingen afvigelser konstateret.

Kontrolmål: 12.6 Sårbarhedsstyring At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
12.6.1	***Styring af tekniske sårbarheder*** Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, virksomhedens eksponering for sådanne sårbarheder evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Inspiceret procedurer for indsamling og vurdering af tekniske sårbarheder. Stikprøvevist inspiceret servere, databaser og arbejdspladser for at konstatere, hvorvidt systemerne er rettidigt patchet i perioden dækket af erklæringen.	Ingen afvigelser konstateret.

Kontrolmål: 13.1 Styring af netværkssikkerhed At sikre beskyttelse af informationer i netværk og beskyttelse af understøttende informationsbehandlingsfaciliteter.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
13.1.2	***Sikring af netværkstjenester*** Netværksservices leveret til cBrain af serviceunderleverandøren Sentia er dækket af en aftale om netværkstjenester. cBrain overvåger og reviderer årligt relevant revisionserklæring fra Sentia.	Inspiceret, at cBrain har indhentet og udført årlig gennemgang af Sentia 3402-erklæring.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 13.1 Styring af netværkssikkerhed At sikre beskyttelse af informationer i netværk og beskyttelse af understøttende informationsbehandlingsfaciliteter.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
13.1.3	***Opdeling af netværk*** Netværk er segregerede.	Inspiceret netværkstegninger, som viser, at netværk hos cBrain og Sentia er segregerede. Stikprøvevist inspiceret implementerede firewall-regler hos Sentia og cBrain med henblik på at konstatere, om de var sat op i overensstemmelse med cBrains politikker.	Ingen afvigelser konstateret.

Kontrolmål: 14.2 Sikkerhed i udviklings- og hjælpeprocesser At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
14.2.2	***Procedurer for styring af systemændringer*** Ændringer af systemer styres ved hjælp af formelle procedurer for ændringsstyring.	Inspiceret proceduren for ændringshåndtering med henblik på at konstatere, om proceduren indeholder krav om: • Godkendelse • Test • Systemdokumentation.	Ingen afvigelser konstateret.
14.2.3	***Teknisk gennemgang af applikationer efter ændringer i driftsplatforme*** Alle ændringer dokumenteres i sagsstyringssystem. Dokumentationen inkluderer information omkring, at ændringer lægges i testmiljø, inden de flyttes til produktionsmiljø.	Inspiceret proceduren for ændringshåndtering. Stikprøvevist inspiceret, om ændringer blev dokumenteret i sagsstyringssystem og dokumentation for at disse lægges i testmiljø, inden de flyttes til produktionsmiljø.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 14.2 Sikkerhed i udviklings- og hjælpeprocesser At sikre, at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
14.2.9	***Systemgodkendelsestest*** Der er udarbejdet kriterier for accept af nye informationssystemer, opgraderinger og nye versioner, og der foretages passende test af systemet(-erne) under udvikling og inden accept af systemet(-erne).	Inspiceret proceduren for ændringshåndtering. Stikprøvevist inspiceret ændringer til F2-systemet fra erklæringsperioden med henblik på at konstatere, om der blev givet systemaccept i overensstemmelse med proceduren. Forespurt om der har været ændringer til M4-system i erklæringsperioden. Inspiceret liste af ændringer i sagsstyringssystem.	cBrain har oplyst, at der ikke er implementeret nye ændringer med relation til M4 i erklæringsperioden. Ingen afvigelser konstateret.

Kontrolmål: 14.3 Testdata At sikre beskyttelse af data, som anvendes til test.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
14.3.1	***Sikring af testdata*** Testdata, der bruges som en del af release test, er anonymiseret og indeholder ingen fortrolige eller personlige oplysninger.	Inspiceret proceduren vedrørende udvælgelse og beskyttelse af testdata. Inspiceret dokumentation fra testmiljøer med henblik på at konstatere, at testdata er anonymiseret og derfor ikke indeholder fortrolige eller personlige oplysninger.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 15.2 Styring af leverandørydelser At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
15.2.1	***Overvågning og gennemgang af underleverandører*** Der evalueres og opdateres en leverandørrisikovurdering på årsbasis. Der indhentes og gennemgås revisionsrapport fra Sentia, og eventuelle relevante rapporterede problemer identificeret i revisionsrapporten registreres og følges op på.	Inspiceret, at revisionsrapport fra Sentia bliver indhentet og gennemgået. Forespurgt, hvorvidt revisionsrapporterne fra underleverandører indeholdt nogle observationer relevante for cBrain. Inspiceret dokumentation for, at der er udført evaluering og opdatering af leverandørrisikovurdering.	Ingen afvigelser konstateret.

Kontrolmål: 16.1 Styring af informationssikkerhedsbrud og forbedringer At sikre en konsekvent og effektiv tilgang til styring af informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og svagheder.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
16.1.1	***Ansvar og procedurer*** Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedshændelser.	Inspiceret, at der er implementeret procedurer for ledelsens hurtige, effektive og planmæssige håndtering af informationssikkerhedshændelser.	Ingen afvigelser konstateret.
16.1.2	***Rapportering af informationssikkerhedshændelser*** Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Inspiceret, at der er implementeret procedurer for registrering og rapportering af mistænkelige sikkerhedssvagheder i systemer og tjenester. Stikprøvevist inspiceret at rapporteringer fra erklæringsperioden til ledelsen, indeholdt information om periodens sikkerhedshændelser. Stikprøvevist inspiceret at registrerede sikkerhedshændelser i log over incidents er registreret af brugerne, overvågningsværktøjer og it-afdelingen.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 16.1 Styring af informationssikkerhedsbrud og forbedringer At sikre en konsekvent og effektiv tilgang til styring af informationssikkerhedshændelser, herunder kommunikation om sikkerhedshændelser og svagheder.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
16.1.3	***Rapportering af sikkerhedssvagheder*** Alle medarbejdere har pligt til at notere og rapportere observerede svagheder eller mistanke om svagheder i relevante systemer.	Inspiceret dokumentation, der viser, at der er implementeret procedurer for registrering og rapportering af svagheder eller mistanke om svagheder i systemer og tjenester. Inspiceret, at der er implementeret log over incidents, hvori brugere kan rapportere om sikkerhedssvagheder.	Ingen afvigelser konstateret.
16.1.6	***At lære af informationssikkerhedsbrud*** Der er etableret mekanismer til at kvantificere og overvåge typer og omfang ved informationssikkerhedsbrud.	Stikprøvevist inspiceret, at ledelsen afholder kvartalsvise møder, hvorpå sikkerhedshændelser evalueres.	Ingen afvigelser konstateret.

Kontrolmål: 17.1 Informationssikkerhedskontinuitet Informationssikkerhedskontinuiteten er forankret i virksomhedens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
17.1.1	***Planlægning af informationssikkerhedskontinuitet*** Der er fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, fx i tilfælde af en krise eller katastrofe.	Inspiceret it-beredskabsplanen for at påse, at den er opdateret, godkendt og behandler de krav, der er nødvendige i forhold til periodiske test.	Ingen afvigelser konstateret.
17.1.2	***Implementering af informationssikkerhedskontinuitet*** Der er fastlagt, dokumenteret, implementeret og vedligeholdt processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation.	Forespurgt, hvorvidt en beredskabsplan er udarbejdet og implementeret dækkende alle it-systemer. Inspiceret it-beredskabsplanen for at konstatere, om it-beredskabsplanen indeholder krav om regelmæssig revurdering til sikring af, at muligheden for reetablering af it-systemer fortsat er til stede.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Kontrolmål: 17.1 Informationssikkerhedskontinuitet Informationssikkerhedskontinuiteten er forankret i virksomhedens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
17.1.3	***Verificer, gennemgå og evaluer informationssikkerheds-kontinuiteten*** It-beredskabsplanerne revideres og testes årligt.	Inspiceret, at beredskabsplaner revideres, og at der er foretaget en årlig skrivebordstest, som omfattede F2- og M4-systemerne.	Ingen afvigelser konstateret.

Kontrolmål: 18.2 Overensstemmelse At sikre, at systemer opfylder kravene i virksomhedens sikkerhedspolitikker og sikkerhedsstandarder.			
Nr.	*Kontrolbeskrivelse*	*Test udført af EY*	*Testresultater*
18.2.2	***Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder*** Ledere sikrer, at sikkerhedsprocedurer inden for deres ansvarsområde efterleves korrekt.	Inspiceret de procedurer, der sikrer, at ledere sikrer overholdelse af sikkerhedspolitikker og sikkerheds-standarder. Forespurgt, om procedurerne er implementeret.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

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."

Robert Lentz
Direktion
På vegne af: cBrain A/S
Serienummer: 6dc38cf6-95f0-4fe9-a814-ca47a9899994
IP: 188.120.xxx.xxx
2024-01-24 14:32:47 UTC

Johanna Sini Annikki Kansonen-Valtersdorf
Statsautoriseret revisor
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: 8af9acce-b73e-4a45-b435-2f7d1272dfaa
IP: 165.225.xxx.xxx
2024-01-24 14:38:48 UTC

Jesper Due Sørensen
EY Godkendt Revisionspartnerselskab CVR: 30700228
Partner
På vegne af: EY Godkendt Revisionspartnerselskab
Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3
IP: 80.208.xxx.xxx
2024-01-24 15:03:47 UTC

Penneo dokumentnøgle: ESTLX-EQNLJ-BNAAY-OMZ5L-HEOM8-6MEKA

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>.** Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**