et trygt samfund med it og data

Revisorerklæring

Clever Choice ApS

ISAE 3402-I erklæring om generelle it-kontroller relateret til driften af ITSM & ESM løsninger pr. 31 januar 2022.

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

Januar 2022

Indholdsfortegnelse

Afsnit 1: Beskrivelse af Clever Choice ApS' generelle it-kontroller i forbindelse med drift af ITSM & ESM løsninger.

I det følgende beskrives Clever Choice ApS' generelle it-kontroller i forbindelse med drift af ITSM & ESM løsninger. Erklæringen omfatter generelle processer og systemopsætninger m.v. hos Clever Choice. Processer og systemopsætninger m.v., der er individuelt aftalt med Clever Choice ApS' kunder er ikke omfattet af erklæringen.

Generelle it-kontroller hos Clever Choice

De løsninger Clever Choice leverer, er tilpasset forskellige typer af kunde. Betingelserne for den enkelte kunde er defineret i kontrakter, hvor det fremgår om løsningen er omfattet af en on premise løsning, eller en løsning hostet af Clever Choice.

Denne erklæring omfatter generelle it-kontroller for de kunder, hvor Clever Choice har ansvaret for hosting af løsningen.

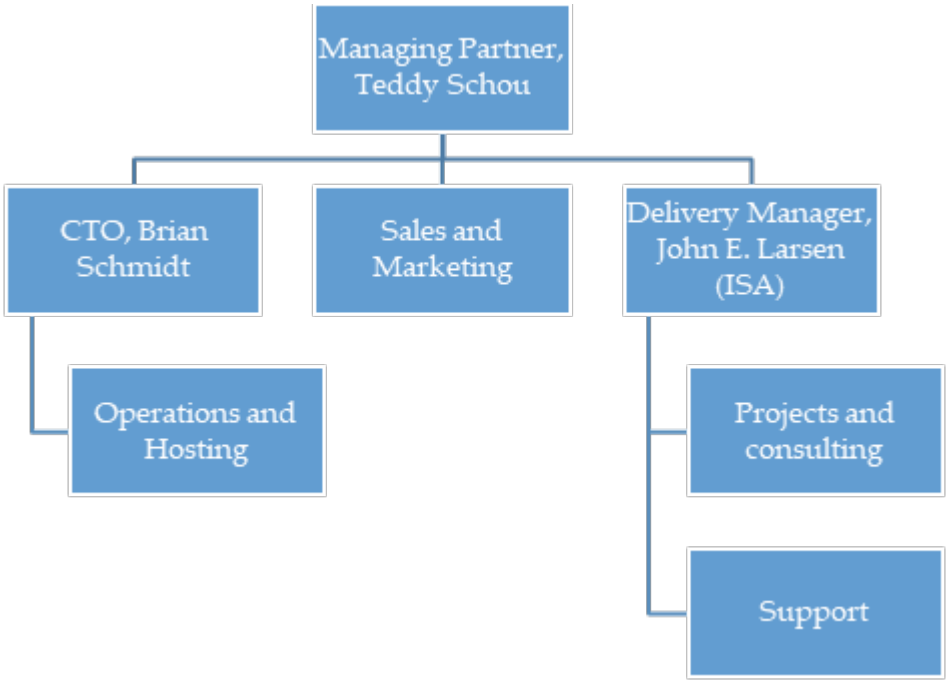
Kontroller i applikationssystemer er ikke omfattet af denne erklæring.

Clever Choice benytter C-Solution som underleverandør på alle hostede løsninger. C-solution er således ansvarlig for den fysiske sikkerhed, hardware, netværk, backup og continuity.

Organisation og ansvar

Clever Choice beskæftiger 16 medarbejdere fordelt på salg, marketing, leverance og support. Leverance og support er ansvarlig for den samlede leverance til kunder, herunder implementering, hosting og support. Support er ansvarlig for hostede miljøer, herunder etablering, drift, overvågning og support.

Ledelsen har det overordnede ansvar for it-sikkerheden i Clever Choice, med direktionen som øverste ansvarlige og ISA (IT sikkerhedsansvarlig) som udførende. Der er indarbejdet kontroller til sikring af, at ledelsen årligt reviderer sikkerhedspolitikken. Øverste ansvarlige leder er Teddy Schou og IT sikkerhedsansvarlig er John E. Larsen



Generelt om risikostyring, kontrolmål og implementerede kontroller

Vi har procedurer for løbende risikovurdering af vores forretning og specielt vores hostede kundemiljøer. Dermed kan vi sikre, at de risici, der er forbundet med hostede kundemiljøer, er minimeret til et acceptabelt niveau.

Risikovurderingen foretages periodisk, samt når der foretages ændringer i systemer eller organisationen, som vi vurderer relevante til at revurdere vores generelle risikovurdering.

Ansvaret for risikovurdering ligger hos den Informationssikkerhedsansvarlige (ISA), og skal efterfølgende forankres og godkendes hos den samlede ledelse.

Vi har defineret vores kvalitetsstyringssystem ud fra vores overordnede målsætning om at levere stabil og sikker it-drift til vores kunder. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartet og gennemsigtig.

Vores it-sikkerhedspolitik er udarbejdet med reference til ovenstående, og er gældende for alle medarbejdere og for alle leverancer.

Vores metodik for implementering af kontroller er defineret med reference til ISO 27001/2:2013 (Regelsæt for styring af informationssikkerhed), og er overordnet inddelt i følgende kontrolområder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Sikkerhed i forhold til HR
- Styring af aktiver
- Adgangskontrol
- Fysisk og miljømæssig sikringer
- Sikkerhed i forbindelse med drift
- Kommunikationssikkerhed
- Leverandørforhold
- Styring af sikkerhedshændelser
- Informationssikkerhedsaspekter ved beredskabsstyring
- Overensstemmelse

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område.

Informationssikkerhedspolitikker

5.1 IT-Sikkerhedspolitik

5.1.1 IT Sikkerhedspolitik dokumenteret

Vi har defineret vores overordnet metodik og tilgang til levering af vores hostede kundemiljøer med hvad det indebærer, i vores it-sikkerhedspolitik og tilhørende strategiske og taktiske dokumenter.

Formålet er at sikre, at vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til vores forretningsstrategi og i forhold til relevant lovgivning.

Dette punkt er yderligere beskrevet tidligere i denne beskrivelse under overskriften ”Generelt om vores kontrolmål og implementerede kontroller”

5.1.2 Evaluering af IT-Sikkerhedspolitikken

Vi opdaterer løbende virksomhedens it-sikkerhedspolitik, og som minimum én gang årligt.

Til mødet omkring revidering af sikkerhedspolitik deltager ISA, CEO samt CTO

6. Organisering af informationssikkerhed

6.1 Intern Organisering

6.1.1 Delegering af ansvar for informationssikkerhed

Vi har en opdelt organisation i funktionsområder, som er beskrevet tidligere i dette dokument. Ansvaret for informationssikkerhed ligger forankret hos virksomhedens samlede ledelse, der sikrer, at alle i organisationen lever op til organisationens vedtaget informationssikkerhed

6.1.2 Funktionsadskillelse

Vores dokumentation, processer og systemer er med til at sikre, at vi udelukker eller minimerer afhængigheden af nøglepersoner.

Funktionsadskillelse er en vigtig del af vores organisation og drift, hvorfor vi, via adgangskontroller og rettighedsstyring, sikrer, at kun autoriseret personale kan udføre de nødvendige handlinger på systemer.

6.1.5 Informationssikkerhed som en del af projektstyring

Vi tager stilling til it-sikkerhed i vores projekter uanset type og størrelse.

6.2 Mobilt udstyr og fjernarbejdspladser

6.2.1 Politik for mobile enheder

Clever Choice har en politik, der danner rammerne for medarbejdernes anvendelse af laptops uden for virksomheden. Dette sikrer at vores laptops er beskyttet i forhold til adgang til hostede løsninger.

6.2.2 Fjernarbejdspladser

Adgang til systemer og dermed potentielt til kundesystemer og data, sker kun for autoriserede personer.

Adgang til hostede miljøer fra hjemmearbejdsplads for vores medarbejdere er sikret via krypteret VPN-forbindelse, hvor bruger skal have lokalt certifikat samt brugernavn og kode for at logge på.

7. Sikkerhed i forhold til HR

7.1 Inden ansættelsen

7.1.1 Screening

Vi har procedurer for ansættelse af medarbejdere og for etablering af samarbejde med eksterne konsulenter, hvor vi sikrer, at vi ansætter den rigtige kandidat i forhold til baggrund og kompetencer. Vi har rolle- og ansvarsbeskrivelser for alle nøglemedarbejdere, så alle er bekendte med deres ansvar

7.1.2 Ansættelsesforhold

Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt.

7.2 Under ansættelsen

7.2.1 Ledelsens ansvar

I forbindelse med ansættelse underskriver nye medarbejdere en kontrakt. I kontrakten er det indeholdt, at den ansatte skal overholde de til enhver tid gældende politikker og procedurer. ligeledes er det klart defineret som en del af kontraktmaterialet, hvad den ansattes ansvar og rolle er.

I forbindelse med anvendelse af eksterne leverandører, som har adgang til vores systemer, er overholdelse af vores politikker og procedurer en del af kontrakten. Relevante politikker er en del af kontrakt materialet og opdateringer eftersendes elektronisk til leverandøren. Vi sikrer på den måde, at leverandører er informeret om relevante ændringer.

7.2.2 Bevidsthed om uddannelse og træning i informationssikkerhed

Der afholdes løbende, dog minimum årligt, awarenesstræning til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med vores informationssikkerhedspolitik

Medarbejdere, og eksterne parter, hvor det er relevant at inkludere disse under vores sikkerhedsretningslinjer, bliver periodisk orienteret om vores sikkerhedsretningslinjer samt når der sker ændringer.

7.2.3 Sanktioner

Der er interne retningslinjer på plads, der sikrer at sanktioner udføres effektivt og rettidigt. Managing Partner og Delivery Manager er øverste myndighed og de eneste, der kan sanktionere.

7.3 Ophør og ændring i ansættelse

7.3.1 Ophør eller ændringer i ansvarsforhold

Generelle vilkår for ansættelse, herunder forhold omkring ophør, er beskrevet i hver medarbejders ansættelseskontrakt. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos den ansattes leder.

Vi har defineret processer og procedurer ved ophør og ændringer i ansættelses og ansvarsforhold der sikrer at adgange bliver ændret/slettet og udleveret udstyr tilbageleveres

8. Styring af aktiver

8.1. Ansvar for aktiver

8.1.1 Fortegnelse over aktiver

Vi har procedure for registrering af servere og hostede kundesystemer i vores interne system, der indeholder alle hostede systemer med tilhørende servere.

8.1.2 Ejerskab af aktiver

Clever Choice benytter sikkerhedsgodkendte leverandører til hosting af alle servere. Hosting leverandører skal årligt levere en ISAE-3402 for at kunne dokumentere at de lever op til forventede krav vedrørende informationssikkerhed.

8.1.3 Acceptabel brug af aktiver

Medarbejdere er i forbindelse med ansættelsen blevet informeret om acceptabelt brug af udleverede aktiver.

8.1.4 Tilbagelevering af aktiver

Ved fratrædelse har vi en procedure, der sikrer at medarbejderen tilbageleverer alle relevante aktiver som er udleveret i forbindelse med ansættelsen. Proceduren sikrer ligeledes, at medarbejderens rettigheder fjernes rettidigt

8.2 Dataklassifikation

8.2.1 Klassifikation af data

Alle data er klassificeret i forhold til at kunne skelne imellem driftssystemer samt test/udviklingssystemer. Denne klassifikation anvendes i forhold til vurdering af backup og tilgængelighed

8.2.2 Mærkning data

Alle data er mærket i vores interne system ved oprettelse. Ved ændring af klassifikation af data bliver dette registreret i vores interne system.

9. Adgangsstyring

9.1 – Forretningskrav til adgangsstyring

9.1.1 – Politikker for adgangsstyring

Vi har politik der sikrer, at kun autoriseret personale har adgang til kundesystemer

9.2 – Administration af brugeradgange

9.2.1 – Brugeroprettelses- og nedlæggelsesprocedure

Ved ansættelse eller ændring i medarbejderens funktion, findes der en procedure, der sikrer at medarbejderen får tildelt de rette godkendte rettigheder

Ved fratrædelse har vi en procedure, der sikrer at medarbejderens rettigheder nedlægges så der ikke længere er adgang til hverken interne systemer eller kundesystemer og kundedata.

9.2.2 – Rettighedstildeling

Tildeling af rettigheder er dækket af vores normale brugeradministrationsproces

9.2.3 – Kontrol med privilegerede adgangsrettigheder

Anvendelse af passwords følger defineret retningslinjer for kompleksitet og fornyelse.

9.2.4 – Håndtering af fortrolige logon informationer

Vi informerer vores medarbejdere i håndtering af fortrolige informationer herunder logon information mv.

9.2.5 – Evaluering af brugeradgangsrettigheder

Der foretages periodisk tjek af, at ingen fratrådte medarbejdere har rettigheder eller adgang til systemer eller data.

9.2.6 – Nedlæggelse eller tilpasning af adgangsrettigheder

Vi har en formel procedure for nedlæggelse og tilpasning af adgangsrettigheder

9.3 – Brugeransvar

9.3.1 – Brug af fortrolige logon informationer

Vores informationssikkerhedspolitik foreskriver, at medarbejderens passwords skal overholde minimumskrav til sikkert password

9.4 – Kontrol af adgang til systemer og data

9.4.1 – Begrænset adgang til data

Medarbejderes adgange til systemer og kundedata er begrænset i henhold til informationssikkerhedspolitikken.

Ingen hostede kunder har adgang til server og databaser. Kunder kan udelukkende tilgå egne data via systemadgang

9.4.2 – Procedurer for sikkert log-on

Der er udelukkende adgang til hostede systemer og kundedata for relevante medarbejdere. Adgang kan udelukkende ske enten direkte via virksomhedens netværk i Roskilde eller alternativt via VPN og sikker adgang på andre lokationer.

9.4.3 – System for administration af adgangskoder

Vi anvender Active Directory til administration af generelle brugerrettigheder. Adgange til hostede systemer og kundedata administreres direkte på de enkelte systemer.

11 – Fysiske og miljømæssige sikringer

11.1 – Sikre områder

11.1.1 – Fysisk skalsikring

Vores lokation er beliggende på 2 sal med adgang udelukkende via hovedindgangen i stuen og ekstra låst adgang på 2 sal. Der er kun adgang for personer med gyldig nøgle og kode til alarmen.

11.1.2 – Fysisk adgangskontrol

Adgang for medarbejdere til vores lokation i Roskilde, kan udelukkende ske med udleveret personlig nøgle. Indgangen til kontormiljøet er altid aflåst.

11.1.3 – Sikring af kontorer, lokaler og faciliteter

Vores lokation i Roskilde er sikret med perimeter sikring samt rumfølere og videoovervågning i relevante lokaler tilkoblet eksternt vagtfirma.

Medarbejdere skal benytte personlig kode for at til- og frakoble alarmen. Alle alarmer og fejlalarmer meldes via eksternt vagtfirma til virksomhedens ISA. ISA har direkte adgang til alarmdata samt historik via app og browser.

12 – Driftssikkerhed

12.1 – Operationelle procedurer og ansvarsområder

12.1.1 – Dokumenterede driftsprocedurer

Vi har igennem vores informationssikkerhedspolitik defineret politikker og procedurer til håndtering af it-drift. Vi sikrer via dokumentationer og procesbeskrivelser – og via kompetente medarbejdere – at alle medarbejdere kan påbegynde et arbejde på et system, som vedkommende ikke har operationel og historisk erfaring med. Vi opererer med dobbeltroller på udvalgte systemer, som sikrer personuafhængighed.

12.1.2 – Ændringsstyring

Vi håndterer alle større eller væsentlige ændringer via vores change proces, således at disse er godkendt og dokumenteret inden idriftsættelsen.

12.1.3 – Kapacitetsstyring

Alle systemer overvåges mht. kapacitet. Der er udarbejdet procedurer til planlægning og overvågning af kapacitet

12.1.4 – Adskillelse af udviklings-, test- og driftsfaciliteter

Kunders produktions, test og udviklingsmiljøer er adskilte og der er etableret nødvendige adgangskontroller for at sikre, at kun autoriseret personale kan tilgå systemer og data

13 – Kommunikationssikkerhed

13.1 Styring af netværkssikkerhed

Al netværkssikkerhed og administration af netværk administreres af ekstern leverandør ud fra virksomhedens retningslinjer

13.2 Informationsoverførsel

Dataoverførsel foretages udelukkende efter aftale med kunden og foretages sikkert mellem kundens miljøer

Der udveksles ikke fortrolige kunde- og persondata via mail og andre åbne medier

15 – Leverandørforhold

15.1 Informationssikkerhed i leverandørforholdet

Netværk samt servere hostes og driftes af eksterne leverandører. Leverandørerne skal leve op til Clever Choices informationssikkerhedspolitik via indgåede aftaler samt løbende opfølgning via regelmæssige driftsmøder og driftsrapportering

16 – Styring af sikkerhedshændelser

16.1 Styring af sikkerhedshændelser

Der er udarbejdet procedurer og kontroller til håndtering af sikkerhedshændelser med fokus på minimal impact på kunder samt undgåelse af kompromittering af kundedata

17 – Informationssikkerhedsaspekter ved beredskabsstyring

Der er udarbejdet procedurer og kontroller til effektiv håndtering af sikkerhedshændelser, der kræver beredskabsstyring, herunder organisering i forhold til ansvar og udførelse af aktiviteter

18 – Overensstemmelse

18.2 Review af informationssikkerheden

Informationssikkerhedspolitikken revideres mindst en gang årligt og relevante risikovurderinger, politikker og procedurer opdateres hvis det findes relevant

Der foretages årligt it-revision via ekstern godkendt kontrollant med henblik på udarbejdelse af en ISAE-3402

Komplementerende kontroller hos kunder

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

Clever Choices kunder er, medmindre andet er aftalt, ansvarlige for:

- At etablere forbindelse til Clever Choices servere. Dette indbefatter, at kunderne selv er ansvarlige for at have en fungerende og tilstrækkelig internetforbindelse samt evt. opsætning og test af alternative internetforbindelser, hvis den primære internetforbindelse skulle fejle
- Regelmæssigt at gennemgå kundens bruger- og systemkonti på applikations-, system- & databaseniveau.
- At alle ændringsanmodninger fra kunden forudsætter en formel godkendelse af ændringsanmodningen. Endvidere skal kunden teste ændringen, inden den kan migreres til produktionsmiljøet.
- Skulle der opstå tvivl om kompromitterede brugerkonti ved f.eks. tyveri af pc, er det kundernes ansvar at informere Clever Choice omgående uden unødvendigt ophold.
- At kunden selv er ansvarlig for udarbejdelse af en beredskabsplan til håndtering af kundens virksomhed i tilfælde af større uheld eller katastrofer.
- At det aftalte niveau for backup dækker kundens behov
- At adgang til miljøer og data er underlagt kundens krav til sikkerhed og at der foreligger procedurer til adgangsstyring hos kunden
- At der opretholdes sporbarhed i tredieparts software som kunden selv administrerer

Afsnit 2: Clever Choice ApS' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt Clever Choice ApS' ITSM & ESM-løsninger, 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.

Clever Choice ApS anvender serviceunderleverandøren C-Solutions ApS. Denne erklæring er udarbejdet efter partielmetoden, og Clever Choice ApS' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos C-Solutions ApS. Enkelte af de kontrolmål, der er anført i Clever Choice ApS' beskrivelse i afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og implementeret sammen med kontrollerne hos Clever Choice ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Clever Choice ApS bekræfter, at:

Den medfølgende beskrivelse i afsnit 1, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for Clever Choice ApS' ITSM & ESM løsninger, der har behandlet kunders transaktioner pr. 31. januar 2022. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne har været udformet og implementeret, herunder redegør for:
- De typer af ydelser, der er leveret.
- De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
- Relevante kontrolmål og kontroller udformet til at nå disse mål.
- Kontroller, som vi med henvisning til kontrollernes udformning har forudsat ville være implementerede af brugervirksomheder, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå.
- Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

(ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget pr. 31. januar 2022.

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

(a) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformede og implementeret pr. 31. januar 2022.

Kriterierne for denne udtalelse var, at:

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

(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

Roskilde, den 2. februar 2022
Clever Choice ApS

John Larsen
Partner & delivery Manager

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

Til Clever Choice ApS, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om Clever Choice ApS' beskrivelse i afsnit 1 af generelle it-kontroller for drift af ITSM & ESM-løsninger og om udformningen og implementeringen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Clever Choice ApS anvender serviceunderleverandøren C-Solutions ApS. Denne erklæring er udarbejdet efter partielmetoden, og Clever Choice ApS' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos C-Solutions ApS.

Enkelte af de kontrolmål, der er anført i Clever Choice ApS' beskrivelse i afsnit 1 af generelle it-kontroller, kan kun nås, hvis de komplementerende kontroller hos kunderne er hensigtsmæssigt udformet og implementeret sammen med kontrollerne hos Clever Choice ApS. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disses komplementerende kontroller.

Clever Choice ApS' ansvar

Clever Choice ApS er ansvarlig for udarbejdelsen af beskrivelsen (afsnit 1) og tilhørende udtalelse (afsnit 2), herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen af kontroller for at nå de anførte kontrolmål.

REVI-IT A/S' uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' internationale retningslinjer for revisorers etiske adfærd (IESBA Code), der bygger på de grundlæggende principper om integritet, objektivitet, professionel kompetence og fornøden omhu, fortrolighed og professionel adfærd, samt etiske krav gældende i Danmark.

REVI-IT anvender ISQC 1[1] og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

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

REVI-IT A/S' ansvar

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

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og implementeringen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes udformning. 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 implementeret.

En erklæringsopgave med sikkerhed af denne type omfatter desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i udtalelsen i afsnit 2.

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

Begrænsninger i kontroller hos en serviceleverandør

Clever Choice ApS' beskrivelse i afsnit 1 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de generelle it-kontroller, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner.

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 Clever Choice ApS' udtalelse i afsnit 2. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var udformet og implementeret pr. 31. januar 2022, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 31. januar 2022

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt Clever Choice ApS' hosting-platform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 2. februar 2022

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
Statsautoriseret revisor

Christian H. Riis
Partner, CISA