Competencehouse A/S

ISAE 3402-erklæring fra uafhængig revisor vedrørende generelle it-kontroller i tilknytning til de ydelser Competencehouse leverer til kunder, der anvender GoDialog.

Indhold

1. Ledelsens udtalelse 3
2. Competencehouses beskrivelse af generelle it-kontroller 4
2.1 Beskrivelse af ydelser, der er omfattet af erklæringen 4
2.2 Kontrolmiljø 4
3. Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet 9
4. Kontrolmål, kontroller, test og resultat heraf 11
4.1 Kontrolmål A: Organisation og informationssikkerhedspolitik 11
4.2 Kontrolmål B: Styring af informationsrelaterede aktiviteter 12
4.3 Kontrolmål C: Fysisk sikkerhed 13
4.4 Kontrolmål D: Logistisk sikkerhed 14
4.5 Kontrolmål E: It-katastrofeberedskab 15

1. Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt GoDialog, 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.

Competencehouse bekræfter, at:

1) Den medfølgende beskrivelse, afsnit 2, giver en retvisende beskrivelse af Competencehouses driftsydelser til kunder, der anvender GoDialog, omfattende behandling af kundernes transaktioner i hele perioden. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

    a) Redegør for, hvordan GoDialog var udformet og implementeret, herunder redegør for:
        - De typer af ydelser, der er leveret, når det er relevant
        - De processer i både it- og manuelle systemer, der er anvendt til at igangsætte, registrere, behandle og om nødvendigt korrigere transaktionerne samt overføre disse til de rapporter, der er udarbejdet til kunder
        - Relevante kontrolmål og kontroller udformet til at nå disse mål
        - Kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret 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 behandlingen og rapporteringen af kunders transaktioner.

    b) Indeholder relevante oplysninger om ændringer i serviceleverandørens system foretaget i perioden 1. januar 2022 - 31. december 2022.

    c) 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 for vigtigt efter dennes særlige forhold.

2) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. januar 2022 - 31. december 2022. Kriterierne for denne udtalelse var, at:

    a) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret
    b) 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
    c) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. januar 2022 - 31. december 2022.

København, den 4. september 2023

Jan Buch
CEO

2. Competencehouses beskrivelse af generelle it-kontroller

2.1 Beskrivelse af ydelser, der er omfattet af erklæringen

Competencehouse leverer cloud-services til ca. 100 offentlige og private kunder. Competencehouses hovedprodukt er systemet GoDialog, der understøtter medarbejderudviklingssamtaler, TUS-samtaler, personalesamtaler, kortlægning af kompetencer, indgåelse af og opfølgning på udviklingsaftaler. Resultaterne gemmes i udviklingsplaner, aftaleoversigter og en række indholds- og processtatistikker. Competencehouse leverer en række varianter af dette system foruden et spørgeskemasystem med tilhørende visning af aktuel resultatstatistik. Endelig kan Competencehouse for kunderne udarbejde rapporter og notater blandt andet med udgangspunkt i data fra kundernes cloud-services.

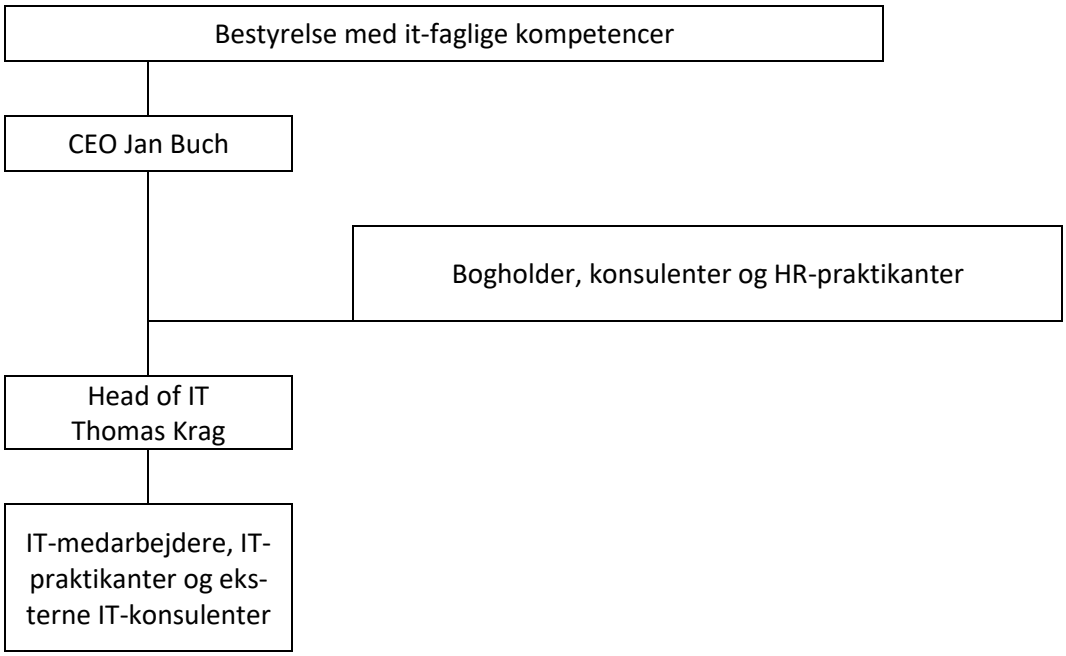
De data, der indgår i Competencehouses cloud-services gemmes "i skyen". I praksis benyttes en driftsserver, som hostes af XDC-gruppen og er fysisk placeret på et datacenter i Danmark. XDC-gruppen får årligt udarbejdet en ISAE 3402-erklæring. De datacentre, som XDC-gruppen benytter sig af, er BFIH-certificerede og får ligeledes årligt udarbejdet en ISAE 3402-erklæring.

2.2 Kontrolmiljø

Organisation og it-informationssikkerhedspolitik

Competencehouse blev etableret i 2000 og har 4 faste medarbejdere foruden en række deltidsansatte, konsulenter og praktikanter.

Organisationsform og ledelse bygger på en funktionsopdelt struktur, hvor CEO har personaleansvaret og har det faglige ansvar for bogholder, konsulenter og HR-praktikanter og Head of IT har det faglige ansvar for it-medarbejdere, it-praktikanter og eksterne it-konsulenter.



Competencehouses it-informationssikkerhedspolitik beskriver de sikkerhedsmæssige foranstaltninger, backup, fordelingen af ansvar mht. sikkerhedspolitikkens overholdelse og beredskabsplanlægning.

CEO har ansvaret for:

1) at Competencehouses informationssikkerhedspolitik opdateres en gang om året i starten af året med det formål at sikre, at politikken lever op til eksterne forpligtigelser udtrykt i lovgivningen og de kontrakter, som Competencehouse har indgået
2) at overvåge og kontrollere, at Head of IT løser de it-sikkerhedsopgaver, Head of IT har ansvar for
3) at informationssikkerhedspolitikken er kendt og efterleves
4) at der ved installation af nye systemer gennemføres en forudgående sikkerheds-/risikovurdering
5) at forebygge sikkerhedsbrud på Competencehouses fjernskriveborde og på Competencehouses interne netværk
6) at Competencehouse har databehandleraftaler fra de leverandører, der har adgang til GoDialog og/eller behandler persondata om Competencehouses kunder og/eller behandler persondata om Competencehouses ansatte
7) at Competencehouses fjernskriveborde kun kan tilgås med et personligt password bestående af mindst 12 karakterer (små/store bogstaver og mindst et tal eller specialtegn). Der er krav om nyt password hvert kvartal
8) at alene Competencehouses fjernskriveborde anvendes til behandling af personfølsomme data fra GoDialog
9) at alle ansatte har underskrevet en opdateret persondataerklæring og fornyer denne en gang om året i starten af året
10) at rapportere kritiske sikkerhedsbrud til Datatilsynet
11) at bortskaffe al it-udstyr på en sikker måde.

Head of IT har ansvaret for:

- at forebygge sikkerhedsbrud på GoDialog
- at der foretages opfølgning på og rapportering af sikkerhedsbrud på GoDialog til direktion og berørte kunder
- at der foretages opfølgning på og rapportering af sikkerhedsbrud hos Competencehouses hostingleverandører til direktion og berørte kunder
- at backup fungerer
- at udskifte adgangskoder til superadministratorindgangen til GoDialog hvert kvartal
- at udskifte adgangskoder til Competencehouses servere hvert kvartal
- at der sker en logning af, hvem der logger på serveren.

Alle ansatte (og tilknyttede, der potentielt kan se og arbejde med kundedata) har ansvar for:

- at overholde informationssikkerhedspolitikken og de regler, der er relevante for den enkeltes arbejdsopgaver
- at gennemlæse og underskrive den persondataerklæring, som Competencehouse udleverer
- at forny deres persondataerklæring en gang om året i starten af året efter anmodning fra ledelsen
- at låse deres computere, når de ikke selv har dem under opsyn
- at opdatere egne adgangskoder til deres Competencehouse fjernskriveborde og e-mail hvert kvartal
- at straks-rapportere mistanke om kunders evt. ulovlige behandling af persondata på GoDialog til Head of IT og CEO
- at straks-rapportere eventuelle sikkerhedsbrud eller mistanke herom relateret til GoDialog til Head of IT
- at straks-rapportere eventuelle andre sikkerhedsbrud eller mistanke herom til CEO'en

Hvis en medarbejder uforsætligt har overtrådt eller forsøgt at overtræde sikkerhedspolitikken eller sikkerhedsreglerne, gives medarbejderen 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 en medarbejder forsætligt overtræder eller forsøger at overtræde sikkerhedspolitikken eller sikkerhedsreglerne, tages der straks skridt til afskedigelse og i særligt grove tilfælde vil der være tale om en bortvisning.

Styring af informationsrelaterede aktiviteter

Medarbejdernes kendskab til Competencehouses it-politik
Alle medarbejdere bliver præsenteret for Competencehouses it-politik ved deres ansættelse og bekræfter deres kendskab til politikken i en persondataerklæring.

Persondata
Ved opsætningen af GoDialog tager den enkelte kunde for kundens version af GoDialog stilling til, hvilke persondata hhv. HR/administratorer, ledere og medarbejdere skal have adgang til og hvilke brugergrupper, der skal have adgang til hvilke persondata.

Competencehouses medarbejdere må ikke ændre en kundes persondataadgangstilladelser uden forudgående skriftlig anmodning herom fra kundens HR-ansvarlige.

De persondata, som Competencehouse behandler for en kunde, fremgår af kundens databehandleraftale.

Adgang til GoDialog er beskyttet af brugernavn og adgangskode og hos visse kunder ved Single Sign-On (SSO) og/eller yderligere sikret ved to-faktor autentifikation. GoDialog sender ingen personfølsomme data ved Single Sign-On. Personfølsom data kan indgå i trafik sendt til GoDialog fra eksterne server(e) som del af Single Sign-On, men denne data sendes krypteret, jvf. afsnit "Kryptering".

Kryptering
Der anvendes kryptering på al ekstern kommunikation til og fra GoDialog. Al kommunikation er krypteret via Competencehouses TLS-certifikat, hvis nøgle er krypteret med RSA, nøglestørrelse 4096 bit. Dette certifikat udskiftes regelmæssigt indenfor en periode på maks. 2 år.

Håndtering af it-problemer
Mål for driftseffektivitet, for svartider og for antal samtidige fejl fremgår af Competencehouses dokument ”Procedure for indberetning og håndtering af it-problemer”, som alle Competencehouses kunder har adgang til. Dokumentet indeholder procedurer for håndtering af forskellige typer af it-problemer samt procedurer for kundernes indberetning af fejl, for kategoriseringen af fejl, for afhjælpningen af fejl samt den løbende dokumentation og afrapportering til kunderne om fremdriften i afhjælpningen.

Den server, der afvikler GoDialog, overvåges løbende, og besked sendes både til Competencehouse og til Competencehouses hostingleverandør ved problemer. Supplerende hermed tjekkes hvert minut, om GoDialog reagerer på en konkret forespørgsel. Er dette ikke tilfældet, modtager Competencehouse besked herom. Hermed sikres, at Competencehouse kan tage aktion i samme øjeblik, at der måtte opstå problemer med GoDialog.

Tilsvarende måles svartider for alle GoDialogs funktioner løbende på serveren.

XDC Gruppen tager daglig backup af den virtuelle driftsserver inklusive databaseserveren (der også ligger på driftsserveren). Backupper gemmes og den enkelte backup overskrives med en ny efter 30 dage. Der er single points-of-failure på al offentlig infrastruktur mellem Competencehouse og XDC.

Backupsystemet indeholder en facilitet, der tester, om den enkelte backup kan indlæses igen, og da atter vil fungere som en server. I supplement hertil foretages mindst én gang årligt et forsøg på en sådan genindlæsning (restore).

Adgangsstyring

Fysisk sikring af Competencehouses lokaler
Competencehouses postadresse er Symbion, hvis lokaler anvendes til møder og lignende, men ikke til egentlige arbejdslokaler, idet størstedelen af arbejdet foretages andetsteds af den enkelte medarbejder via fjernskrivebords-adgang. Der er derfor ikke behov for fysisk sikring og overvågning af Symbions lokaler.

Fysisk sikring af Competencehouses servere
Competencehouse har virtuelle servere, som er placeret på XDC-gruppens hostinglokation. XDC-gruppens hostinglokation har en fysisk sikkerhed, som er revideret efter ISAE 3402 Type 2.

XDC-gruppens hostinglokation er således:

- sikret med elektronisk låsesystem/alarm således, at kun autoriserede personer har adgang
- etableret med ydervægge, døre, vinduer mv. som er eksponeret mod uautoriseret adgang.

Overvågning og beskyttelse af serverne sker mod:

- uautoriseret indtrængning ved anvendelse af elektronisk låsesystem
- strømudfald således, at udstyret kan lukkes behørigt ved længerevarende strømsvigt
- brand ved anvendelse af godkendt branddetekterende og brandbekæmpende udstyr
- overophedning ved anvendelse af aktiv køling (aircondition)
- vand som følge af brud på rør eller indtrængende vand fra kloakker mv. (er forebygget via placering og indretning af lokalerne ved anvendelse af fugtfølere).

Overvågning og beskyttelsesudstyr bliver periodisk gennemset og testet af en autoriseret leverandør.

Logistisk adgangskontrol i Competencehouse
For at styre medarbejdernes adgang til GoDialog og til Competencehouses fjernskrivebord er der etableret adgangsregler og -rettigheder.

Medarbejderadgang til GoDialog sker gennem et administrationsinterface, der er tilgængeligt online.

Medarbejderadgang til Competencehouses fjernskrivebord er underlagt firmaets adgangskodepolitik.

Både administrationsinterface og fjernadgang gør brug af to-faktor autentifikation.

Logistik adgangskontrol for brugere af GoDialog
Det sikres, at:

- brugerlogin (både succesfulde og fejlede) logges
- ovennævnte logninger gennemgås periodisk, enten manuelt eller automatisk ved hjælp af værktøjer
- loggen gemmes minimum 5 år.

Beredskab

Katastrofer søges undgået gennem fysisk sikring og overvågning af bygninger og tekniske installationer samt ved overvågning af Competencehouses servere og af trafikken på GoDialog. Da såvel kundernes data som Competencehouses persondata ligger på eksternt placerede servere på XDC-gruppens hostinglokation i Danmark, vil en katastrofe andetsteds ikke berøre kundernes data.

Competencehouses servere
XDC-gruppen har et it-katastrofeberedskab, som sikrer, at XDC i tilfælde af større driftsnedbrud eller egentlige katastrofer er i stand til at genoptage kritiske forretningsaktiviteter efter en forud defineret tidshorisont. XDC gennemfører mindst en gang pr. år en egenkontrol af it-katastrofeberedskabet.

GoDialog nedbrud
I tilfælde af GoDialog nedbrud har Competencehouse etableret en linje til orientering af alle leverandører. Al logning har backups hos XDC Gruppen. Da der tages fuld backup af server og database dagligt, vil der i allerværste tilfælde højst mistes data for 1 dag.

Ved nedbrud af GoDialog eller ved overtrædelse af fastsatte tærskelværdier for antallet af kritiske fejl, for driftseffektivitet og/eller for svartider er der etableret et beredskab, som indebærer:

1. at CEO straks-orienteres af Head of IT
2. at berørte kunders GoDialog administratorer orienteres hurtigst muligt
3. at CEO vurderer behovet for/træffer beslutning om:
   a) afholdelse af eskalationsmøde
   b) allokering af ekstra evt. eksterne ressourcer til at udbedre fejl, optimere driftseffektiviteten og/eller svartiderne
   c) tidsplan for udbedringsopgaven
   d) mødeplan for statusopfølgning på udbedringsopgaven
   e) rapportering til Competencehouses bestyrelse og hvis relevant til Datatilsynet
   f) udvidet information til berørte kunder, herunder hvor hyppigt der skal gives en orientering, og hvem der skal kontaktes: Kundernes CEO, økonomidirektør, it-chef, HR-chef og/eller GoDialog administratorer.

Hacking og virusangreb

Der er etableret kontroller til beskyttelse mod malware og lignende skadelig kode.
Der er etableret kontroller både i Competencehouse og i XDC-gruppen af forsøg på at hacke GoDialog. Alle forsøg på hacking og virusangreb er afværget som følge af kontrollen.

3. Serviceleverandørs uafhængige revisors erklæring med sikkerhed om beskrivelse af kontroller, deres udformning og funktionalitet

Til serviceleverandøren Competencehouse A/S

Omfang

Vi har fået til opgave at afgive erklæring om Competencehouse A/S's beskrivelse i afsnit 2 af leveringen af GoDialog og om udformningen og funktionen af generelle it-kontroller, der vedrører regnskabsaflæggelsen, i relation til de kontrolmål, som er anført i beskrivelsen for perioden 1. januar 2022 - 31. december 2022.

Competencehouse A/S' ansvar

Competencehouse A/S er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af GoDialog, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Vores uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske Regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd. Firmaet anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

Serviceleverandørens revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om serviceleverandør Competencehouse A/S's 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 overholder etiske krav samt 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 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 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

Competencehouse A/S beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og disses revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved systemet, som hver enkelt kunde måtte anse for vigtigt efter dennes 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 funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i afsnit 1. Det er vores opfattelse:

a) at beskrivelsen af GoDialog, således som den var udformet og implementeret i hele perioden 1. januar 2022 - 31. december 2022, 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 udformet i hele perioden 1. januar 2022 - 31. december 2022.
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 fungeret effektivt i hele perioden 1. januar 2022 - 31. december 2022.

Beskrivelse af test af kontroller

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

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i afsnit 4 er udelukkende tiltænkt kunder, der har anvendt GoDialog i perioden 1. januar 2022 - 31. december 2022 og disses 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.

Rødovre, den 4. september 2023.
REVISOR-FÆLLESSKABET af 1976 ApS
CVR-nr. 57 98 17 17

Jan V. Hansen (mne454)
Registreret revisor

4. Kontrolmål, kontroller, test og resultat heraf

4.1 Kontrolmål A: Organisation og informationssikkerhedspolitik

Der er etableret passende forretningsgange og kontroller for opretholdelse af det aftalte sikkerhedsniveau hos Competencehouse. A/S

Kontrolmål/kontrol	REVISOR-FÆLLESSKABETs test	Resultat af REVISOR-FÆLLESSKABETs test
Skriftlig politik for informationssikkerhed Ledelsen har dokumenteret et sæt af politikker for informationssikkerhed, som gennemgås og vedligeholdes mindst en gang årligt samt i tilfælde af væsentlige ændringer. Sikkerhedspolitikken er godkendt af bestyrelsen.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at bestyrelsen har godkendt sikkerhedspolitikken, samt at den opdateres løbende.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsens forpligtigelse i forbindelse med informationssikkerhed De organisatoriske ansvarsområder for informationssikkerhed, herunder ansvar og roller, er defineret i sikkerhedspolitikken. Endvidere er der fastlagt regler for fortrolighedsaftaler og rapportering om informationssikkerhedshændelser.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Vi har endvidere fortaget inspektion af, at fortrolighedsaftaler og rapportering om informationssikkerhedshændelser er udarbejdet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Underleverandører Identifikation af risici sker i relation til XDC-gruppen herunder håndtering af sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til kunder.	Vi har forespurgt ledelsen om de kontrolaktiviteter, der foretages. Vi har inspiceret, at XDC-gruppen har en ISAE 3402-erklæring og en databehandleraftale, der omfatter at databehandleren handler efter instruks fra Competencehouse og indeholder bestemmelser om fortrolighed og behandlingssikkerhed.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

4.2 Kontrolmål B: Styring af informationsrelaterede aktiviteter

Der er implementeret passende foranstaltninger til sikring af medarbejdernes kendskab til og ansvar for Competencehouses it-sikkerhed.

Kontrolmål/kontrol	REVISOR-FÆLLESSKABETs test	Resultat af REVISOR-FÆLLESSKABETs test
Information om sikkerhedspolitikken Medarbejderne i Competencehouse er informeret om den gældende sikkerhedspolitik. Medarbejderne bliver ved deres ansættelse præsenteret for Competencehouses sikkerhedspolitik (it-sikkerhedspolitik og privatlivsbeskyttelsespolitik) og underskriver en persondataerklæring om, at de vil efterleve de forskellige regler.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret det program, hvor medarbejderne bliver præsenteret for sikkerhedspolitikken og har kontrolleret, at alle medarbejdere har underskrevet en persondataerklæring.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Fortrolighed Medarbejderne er pålagt tavshedspligt over for tredjemand. Den persondataerklæring, som medarbejderne underskriver, indeholder en erklæring om tavshedspligt.	Vi har inspiceret, at persondataerklæringerne indeholder en erklæring om tavshedspligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Håndtering af it-problemer Alle kunders HR-chef/GoDialog administratorer har adgang til "Procedure for indberetning og håndtering af it-problemer", som indeholder procedurer for kundernes indberetning af fejl, for kategoriseringen af fejl, for afhjælpningen af fejl samt den løbende dokumentation og afrapportering til kunderne. Opståede problemer dokumenteres løbende.	Vi har inspiceret den skriftlige procedure for indberetning og håndtering af it-problemer og har kontrolleret, at alle kunder har adgang til proceduren, og at den indeholder de forhold, Competencehouse har beskrevet. Vi har stikprøvevis inspiceret, at it-problemer dokumenteres og at kunderne orienteres herom.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

4.3 Kontrolmål C: Fysisk sikkerhed

Den fysiske sikkerhed er passende dokumenteret og implementeret.

Kontrolmål/kontrol	REVISOR-FÆLLESSKABETs test	Resultat af REVISOR-FÆLLESSKABETs test
Fysisk sikring af Competencehouses lokaler Competencehouse anvender mødelokaler i Symbion, men ikke til egentlige arbejdslokaler, idet størstedelen af arbejdet foretages andetsteds af den enkelte medarbejder via fjernskrivebords-adgang. Der er derfor ikke behov for fysisk sikring og overvågning af Symbions mødelokaler.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres i forbindelse med anvendelse, opdatering og rotering af adgangskoder til Competencehouses VPN-forbindelser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Fysisk sikring af hostingcenters lokaler Lokalerne er sikret med elektronisk låsesystem/alarm, således at kun autoriserede personer har adgang. Ydervægge, døre, vinduer mv. er eksponeret mod uautoriseret adgang. Der sker en overvågning og beskyttelse af servere mod strømudfald, brand, overophedning og indtrængning af vand. Competencehouse modtager en 3402 erklæring fra XDC-gruppen hvert år til gennemgang og kontrol af den fysiske sikring.	Vi har inspiceret, at den modtagne ISAE 3402 erklæring for XDC-gruppen for perioden 1. januar 2021 - 31. december 2021 omfatter Competencehouses beskrivelse af den fysiske sikring af hostingcenters lokaler og servere.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

4.4 Kontrolmål D: Logistisk sikkerhed

Den logistiske adgangskontrol er passende dokumenteret og implementeret.

Kontrolmål/kontrol	REVISOR-FÆLLESSKABETs test	Resultat af REVISOR-FÆLLESSKABETs test
Logning af brugeraktivitet på GoDialog Competencehouse logger aktiviteter gennem centrale logningsværktøjer. Login hændelser for brugere registreres, både succesfulde og fejlede. Logningerne gennemgås periodisk.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har stikprøvevis inspiceret, at systemopsætningen af parametre for logning er opsat således, at handlinger udført af både succesfulde og fejlede logninger bliver registreret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Passwordsikkerhed Competencehouse har en nedskrevet passwordpolitik, som alle medarbejdere bliver gjort bekendt med ved udarbejdelsen af deres persondataerklæring.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres i forbindelse med passwordkontroller og har inspiceret, at der anvendes passende autentifikation af brugere på alle adgangsveje. Vi har inspiceret, at alle medarbejdere har underskrevet en persondataerklæring, hvor passwordpolitikken er beskrevet. Vi har ved stikprøvekontrol inspiceret, at der anvendes en passende passwordkvalitet på Competencehouses fjernskriveborde og i GoDialogs driftsmiljø.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

4.5 Kontrolmål E: It-katastrofeberedskab

Der er etableret et passende it-katastrofeberedskab

Kontrolmål/kontrol	REVISOR-FÆLLESSKABETs test	Resultat af REVISOR-FÆLLESSKABETs test
GoDialog-nedbrud Ved nedbrud af GoDialog er der etableret et beredskab, som indebærer • at CEO straks-orienteres af Head of IT • at berørte kunders GoDialog-administratorer orienteres hurtigst muligt • at der igangsættes en eskalationsprocedure for løsning af problemerne herunder allokering af ekstra ressourcer.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres. Vi har inspiceret, at der er udarbejdet en beredskabsplan, der indeholder procedurer for straks-orientering af CEO, orientering af kunder og udarbejdelse af en plan for løsning af problemerne. Vi har inspiceret at beredskabsplanen er beskrevet i notatet "Procedurer for indberetning og håndtering af it-problemer", som Competencehouses kunder har adgang til.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Katastrofeberedskab-servere XDC-gruppen har et it-katastrofeberedskab som sikrer, at XDC i tilfælde af katastrofer er i stand til at genoptage kritiske forretningsaktiviteter efter forud defineret tidshorisont. XDC gennemfører mindst en gang pr. år en egenkontrol af it-katastrofeberedskabet. Competencehouse modtager en 3402 erklæring fra XDC-gruppen hvert år til gennemgang og kontrol af katastrofeberedskabet.	Vi har inspiceret, at den modtagne ISAE 3402 erklæring for XDC-gruppen for perioden 1. januar 2022 - 31. december 2022 omfatter et katastrofeberedskab, omfattende de forhold Competencehouse har beskrevet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Hacking af GoDialog Der er etableret kontroller til at identificere forsøg på hacking af GoDialog.	Vi har forespurgt ledelsen om de procedurer og kontrolaktiviteter, der udføres og fået oplyst, at alle forsøg på hacking og virusangreb er afværget som følge af kontrollen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

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."

Jan Buch
CEO
Serienummer: 86d98eb2-445a-49c8-bbc9-daeafba743ce
IP: 45.10.xxx.xxx
2023-09-06 07:16:02 UTC

Mit ID

Jan Valther Hansen
Registreret revisor
Serienummer: b7298087-14a8-45c0-b38c-4799a3970aec
IP: 94.18.xxx.xxx
2023-09-06 07:46:13 UTC

Mit ID

Penneo dokumentnøgle: 837SE-QDK1I-PQPLQ-PAT4B-QHO7T-M5CWH