Procopa IT

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller pr. 8 marts 2023 i relation til hosting aktiviteter i Procopa IT´s hostingmiljø, som benyttes til private cloud hosting for Procopa IT's kunder

Marts 2023

Indholdsfortegnelse

1 Ledelsens udtalelse

Medfølgende beskrivelse er udarbejdet til brug for Procopa IT's kunder, der har anvendt hosting aktiviteter i Procopa IT´s hostingmiljø, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som Procopa IT's kunder selv har anvendt ved vurdering af risiciene for væsentlig fejlinformation i Procopa IT's kunders regnskaber.

Procopa IT anvender CibiCom og GlobalConnect som serviceunderleverandør for hosting. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som CibiCom og GlobalConnect varetager for Procopa IT.

Enkelte af de kontrolmål, der er anført i vores beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunder er hensigtsmæssigt udformet sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen af disse komplementære kontroller.

Procopa IT bekræfter, at:

a) Den medfølgende beskrivelse i afsnit 3 giver en tilfredsstillende præsentation af hosting aktiviteter i Procopa IT´s hostingmiljø, der har behandlet kunders transaktioner pr. 8 marts 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan generelle it-kontroller i relation til hosting aktiviteter i Procopa IT´s hostingmiljø var udformet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret
   - De processer i både it-systemer og manuelle systemer, der er anvendt til styring af generelle it-kontroller
   - Relevante kontrolmål og kontroller udformet til at nå disse mål
   - Kontroller, som vi med henvisning til hosting aktiviteter i Procopa IT´s hostingmiljøs 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
   - Hvordan andre betydelige begivenheder og forhold end transaktioner behandles
   - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller

   (ii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne generelle it-kontroller i relation til hosting aktiviteter i Procopa IT´s hostingmiljø, 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 generelle it-kontroller i relation til hosting aktiviteter i Procopa IT´s hostingmiljø, som den enkelte kunde måtte anse vigtigt efter sine særlige forhold.

b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 8 marts 2023. Kriterierne anvendt for at give denne udtalelse var, at:

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

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

Daniel Lundbye
Brøndby
21 marts 2023

2 Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller og deres udformning

Uafhængig revisors ISAE 3402-erklæring vedrørende generelle it-kontroller pr. 8 marts 2023 i relation til hosting aktiviteter i Procopa IT´s hostingmiljø, som benyttes til private cloud hosting for Procopa IT's kunder.

Til: Procopa IT og Procopa IT's kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om Procopa IT's beskrivelse i afsnit 3 af deres generelle it-kontroller i relation til hosting aktiviteter i Procopa IT´s hostingmiljø, der har behandlet kunders transaktioner pr. 8 marts 2023, og om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Procopa IT anvender CibiCom og GlobalConnect som serviceunderleverandør for hosting. Erklæringen anvender partielmetoden og omfatter ikke kontrolmål og tilknyttede kontroller, som CibiCom og GlobalConnect varetager for Procopa IT.

Enkelte af de kontrolmål, der er anført i Procopa IT's beskrivelse i afsnit 3, kan kun nås, hvis de komplementære kontroller hos kunder er hensigtsmæssigt udformet sammen med Procopa IT's kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen af disse komplementære kontroller.

Vi har ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

Procopa IT's ansvar

Procopa IT er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udtalelse i afsnit 1, 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 og implementeringen kontroller for at opnå de anførte kontrolmål.

Revisors 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.

PricewaterhouseCoopers 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.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om Procopa IT's beskrivelse samt om udformningen af de 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 de yderligere krav, der er gældende i Danmark. Denne standard kræver, at vi planlægger og udfører vores handlinger med henblik på at opnå høj grad af

sikkerhed for, at beskrivelsen i alle væsentlige henseender er tilfredsstillende præsenteret, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sin hosting aktiviteter i Procopa IT´s hostingmiljø samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er tilfredsstillende præsenteret, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål samt hensigtsmæssigheden af de kriterier, som Procopa IT har specificeret og beskrevet i ledelsens udtalelse.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende funktionaliteten af de kontroller, der indgår i afsnit 4, og udtrykker derfor ingen konklusion herom.

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

Procopa IT's 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 hosting aktiviteter i Procopa IT´s hostingmiljø, som hver enkelt kunde måtte anse for vigtige efter sine 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.

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 ledelsens udtalelse. Det er vores opfattelse,

a) at beskrivelsen af de generelle it-kontroller i relation til hosting aktiviteter i Procopa IT´s hostingmiljø, således som de var udformet og implementeret pr. 8 marts 2023, i alle væsentlige henseender er tilfredsstillende præsenteret, og

b) at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 8 marts 2023.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, samt arten, den tidsmæssige placering og resultaterne af disse test 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 Procopa IT's hosting aktiviteter i Procopa IT´s hostingmiljø, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundernes egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

Århus, den 21. marts 2023
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 77 12 31

Jesper Parsberg Madsen
statsautoriseret revisor
mne26801

3 Beskrivelse af behandling

3.1 Introduktion

Beskrivelsen af generelle IT-kontroller vedrører hosting aktiviteter i Procopa IT´s hostingmiljø, som benyttes til private cloud hosting for Procopa IT's kunder.

Herudover for Procopa IT's shared hosting miljø for e-mail og Cloudstore.

Der anvendes underleverandører til fysiske datacentret. Disse leverandører er ansvarlige for den fysiske sikkerhed i datacentrene.

Procopa IT ejer egen infrastruktur og benytter sig kun af underleverandører på Co-Loacation, fiberkapaciteter og spamfilter.

3.2 Vision

Procopa IT's kerneforretning er at agere outsourcede IT-afdeling og primære hostingpartner for små og mellemstore virksomheder.

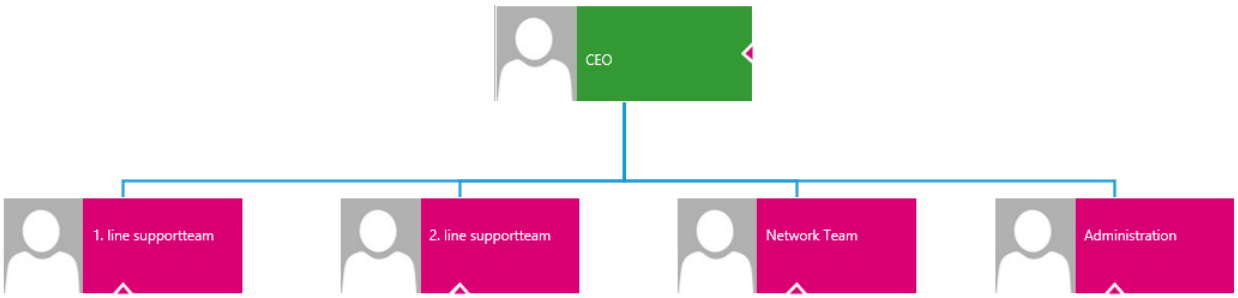
Procopa IT stiller en hosting platform tilrådighed, som kan sikre kunders data altid er i Danmark. Procopa IT arbejder ud fra en målsætning om at kunne være totalleverandør af infrastruktur, hosting og support med base i Danmark.

3.3 Organisation

Procopa IT er stiftet i 2012. Procopa IT ledes til dagligt af CEO Daniel Lundbye.

Organisationen består af et supportteam og et administrationsteam.

Supportteamet er opdelt i 1. line-, 2. line- og netværkskonsulenter.



3.4 Informationssikkerhedspolitikker

Formålet med Procopa IT's informationssikkerhedspolitik er at sikre, at Procopa IT altid følger god it-praksis og overholder gældende lovgivning, og at Procopa IT's medarbejder- og kundedata altid er beskyttet.

Informationssikkerhedspolitikken revideres løbende og mindst én gang årligt, eller når nye systemer, services, forretningsprocesser mv., der påvirker informationssikkerheden, introduceres.

Informationssikkerhedspolitikken definerer omfanget, ansvaret og styringen af informationssikkerhed hos Procopa IT.

Kritiske informationssystemer skal identificeres og beskyttes ordentligt mod brud på tilgængelighed, integritet og fortrolighed.

Risici skal reduceres til et kendt og acceptabelt niveau, og overholdelse af gældende lovgivning skal til enhver tid sikres.

Beskyttelsesniveauet og relaterede omkostninger skal baseres på en forretningsrelateret risiko- og Procopa IT's vurdering, som skal udføres mindst én gang om året.

3.5 Organisering af informationssikkerhed

Procopa IT's direktion har det ultimative ansvar for informationssikkerheden.

Hos Procopa IT vurderes it-sikkerheden løbende, og risikovurderinger opdateres løbende. Endvidere vurderes det løbende, om de tilknyttede informationssikkerhedspolitikken, opfylder eksterne forpligtelser fastsat ved lov og i kontrakter eller aftaler.

Informationssikkerhedspolitikken udleveres til alle nye medarbejdere på ansættelsestidspunktet for at sikre, at alle medarbejdere er opmærksomme på Procopa IT's retningslinjer. Politikken indeholder blandt andet retningslinjer for mobile enheder. Opdateringer af politikken eller procedurer formidles til de relevante medarbejdere via mail og på interne møder.

Hvert år indhenter Procopa IT attesteringsrapporter eller relevant dokumentation om underleverandører, der anses for at være kritiske.

3.6 Medarbejdersikkerhed

Procopa IT's ledelse er ansvarlig for at sikre, at alle medarbejdere er tilstrækkeligt informeret om deres roller og ansvar ved brug af Procopa IT's it-systemer, at de er blevet gjort opmærksomme på de nødvendige politikker og procedurer, og at de overholder dem i deres daglige arbejde.

Ethvert brud på eller forsøg på brud på Procopa IT's informationssikkerhedsregler og -procedurer kan have ansættelsesretlige konsekvenser, som vil blive pålagt efter en samlet vurdering af bruddets alvor og karakter.

Ved ansættelsen foretages screening, og der opnås relevante legitimationsoplysninger. I betragtning af den rolle, kandidaten skal udfylde, kan hans eller hendes straffeattest indhentes.

3.7 Asset Management

Procopa IT har overblik over virksomhedens samlede informationsaktiver.

Gennem informationssikkerhedspolitikken informeres Procopa IT's medarbejdere om den acceptable brug af udstyr, der stilles til rådighed. Ved ansættelsens ophør sker returnering af udstyr til Procopa IT

Enheder, der stilles til rådighed af Procopa IT, er krypterede, og medarbejderne informeres om sikker brug af USB-enheder, f.eks. gennem informationssikkerhedspolitikken.

3.8 Adgangsstyring

Der er etableret processer for at sikre en korrekt tildeling af adgangsrettigheder til Procopa IT's data og it-systemer.

Der udføres periodisk gennemgang af bruger- og adgangsrettigheder.

Interne- og driftsmiljøer kan tilgås Procopa IT's kontor eller via en sikker VPN-forbindelse.

Brugerkonti til brug for adgang til VPN og Microsoft 365 er underlagt Multi Factor Authentication (MFA).

3.9 Kryptering

Kryptering bruges på medarbejder-pc'er, og dekrypteringsnøgler opbevares i Procopa IT's AD.

Kundemiljøer kan kun tilgås via en VPN-forbindelse, som er beskyttet af MFA

3.10 Fysisk og system sikkerhed

Underleverandørerne Global Connect og Cibicom er ansvarlige for den fysiske sikkerhed i datacentrene.

Informationsaktiver i alle lokaler er beskyttet af fysisk adgangskontrol, og medarbejdere og eksterne parter har adgang via personlige adgangskort.

3.11 Driftssikkerhed

Procopa IT har en række procedurer for f.eks. oprettelse af servere, overvågning og backup for at standardisere driften.

Drift og kundemiljøer er adskilt for at reducere risikoen for uautoriseret adgang.

Procopa IT installerer software på enheder og servere efter instrukser fra kunder, og relevante medarbejdere underrettes om eventuelle opdateringer eller ændringer som er relevant for driften.

Ressourcer som CPU, RAM, ledig diskplads osv. overvåges på alle kundeløsninger for at sikre, at den nødvendige kapacitet er tilgængelig.

Sikkerhedskopiering af operativsystemer foretages automatiseret hver måned.

Sikkerhedsopdatering eller versionsopdatering af kundespecifikke applikationer i kunders egne afgrænsede miljøer foretages efter aftale med kunder og eventuelle systemleverandører til kunder.

Antivirus software installeres på kundeservere i det omfang det ønskes af kunderne.

3.12 Kommunikationssikkerhed

Procopa IT inkorporerer fortrolighed i handelsaftaler og opretter tavshedspligt, når det er nødvendigt. Om nødvendigt er medarbejderne underlagt udvidet tavshedspligt. Fortrolige data sendes gennem sikre kommunikationskanaler som krypteret e-mail eller gennem sikker overførsel.

3.13 Leverandørforhold

Procopa IT anvender kun leverandører godkendt af direktionen.

Freelancere, der arbejder på Procopa IT's systmer, skal overholde Procopa IT's informationssikkerhedspolitik.

Endvidere gennemføres en løbende inspektion af alle leverandører, der fungerer som databehandlere/underdatabehandlere for Procopa IT.

Dette gøres ved at indhente relevante erklæringer / certificeringer / standarder eller ved en formaliseret indsamling af information i skriftlig form.

Alle leverandører gennemgås løbende for at vurdere, om leverandørerne stadig leverer en relevant ydelse til Procopa IT.

3.14 Hændelseshåndtering

Procopa IT's direktion har det overordnede ansvar for hændelsesstyring.

Alle medarbejdere er forpligtet til at indberette observerede eller formodede svagheder i it-systemer eller tjenester til direktionen. Direktionen bruger den viden, der opnås ved at analysere og håndtere brud på informationssikkerheden, til at reducere risikoen for fremtidige brud.

3.15 Overholdelse

Procopa IT holder sig ajour med relevant lovgivning og praksis, der kan have indflydelse på virksomheden. Direktionen vurderer, om der er behov for nye tiltag eller ændringer som følge heraf.

Procopa IT's kundeløsninger er baseret på instruktioner fra vores kunder, og den enkelte kunde er forpligtet til at holde Procopa IT orienteret, hvis den bliver påvirket af nye lovkrav eller ændret praksis af betydning for Procopa IT's leverancer.

Eventuelle andre særlige krav håndteres af det fortsatte kontraktforhold.

Procopa IT sikrer, at en årlig revision udføres af en ekstern revisor.

Overholdelse af politikker og standarder sikres af direktionen, som blandt andet vurderer værdien af bevidstgørelsestræningen for medarbejderne. Der udføres en række kontroller og stikprøver af den faktiske overholdelse. I den forbindelse vurderes det også, om der er behov for yderligere tiltag for at afbøde nye risici.

4 Kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

4.1 Formål og omfang

Vi har udført vores arbejde 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 kontrollernes design og implementering har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen, og som fremgår af afsnit 4.3. Eventuelle andre kontrolmål, tilknyttede kontroller og kontroller hos kunder er ikke omfattet af vores testhandlinger.

Vores test af design og implementering har omfattet de kontrolaktiviteter, som blev vurderet nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået.

4.2 Testhandlinger

De udførte testhandlinger i forbindelse med fastlæggelsen af kontrollers design og implementering er beskrevet nedenfor:

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse af 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 være effektive, hvis de implementeres. Endvidere vurderes det, om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel af relevant personale. Forespørgsler har omfattet, hvordan en kontrol udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.3 Oversigt over kontrolmål, kontrolaktivitet, testhandlinger og resultat heraf

Kontrolmål: Informationssikkerhedspolitik

Ledelsen har udarbejdet en informationssikkerhedspolitik, som udstikker en klar målsætning for it-sikkerhed, herunder valg af referenceramme samt tildeling af ressourcer. Informationssikkerhedspolitikken vedligeholdes under hensyntagen til en aktuel risikovurdering.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
A.1	**Skriftlig politik for informationssikkerhed** Procopa IT har udarbejdet en sikkerhedspolitik. Denne er til rådighed for medarbejdere på intranettet. Den revideres mindst én gang årlig. Den er godkendt af ledelsen	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at ledelsen har godkendt sikkerhedspolitikken, samt at den som minimum er revurderet én gang årligt. Endvidere har vi påset, at den forefindes let tilgængelig for medarbejderne.	Vores test har ikke ført til bemærkninger.
A.2	**Ledelsens forpligtelse vedrørende informationssikkerhed** Det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Endvidere er der fastlagt regler for fortrolighedsaftaler og rapportering af informationssikkerhedshændelser samt udarbejdet en fortegnelse over aktiver.	Vi har forespurgt om ledelsens roller og ansvar. Vi har påset, at der anvendes fortrolighedsaftaler og rapportering af sikkerhedshændelser.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Organisering af informationssikkerhed

Det organisatoriske ansvar for informationssikkerhed er passende dokumenteret og implementeret, ligesom håndtering af eksterne parter sikrer en tilstrækkelig behandling af sikkerhed i aftaler.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
B.1	**Ledelsens forpligtelse i forbindelse med informationssikkerhed** Ledelsen er ansvarlig for, at nye medarbejdere gøres bekendt med retningslinjerne som en del af introduktionen til virksomheden. I takt med at der sker opdatering af retningslinjerne, vil der blive givet besked herom via mail, hvor man også kan finde den ajourførte og gældende version af sikkerhedspolitikken.	Vi har overordnet drøftet styring af informationssikkerhed med ledelsen. Vi har påset, at det organisatoriske ansvar for informationssikkerhed er dokumenteret og implementeret. Endvidere har vi foretaget inspektion af, at rapportering om informationssikkerhedshændelser samt fortegnelse over aktiver er udarbejdet.	Vores test har ikke ført til bemærkninger.
B.2	**Eksterne parter** Procopa IT beder samarbejdspartnere og eksterne leverandører om at underskrive en kontrakt, der beskriver fortrolighed og sikkerhedsforanstaltninger. Procopa IT sikrer, at eksterne partnere er bekendt med Procopa IT's sikkerhedspolitik.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har påset, at der er etableret betryggende procedurer for samarbejde med eksterne leverandører. Vi har desuden stikprøvevis kontrolleret, at samarbejdet med eksterne parter er baseret på godkendte kontrakter og vi har påset, at der er modtaget revisorerklæring fra backupleverandører for den relevante periode.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Fysisk sikkerhed

Driftsafviklingen foregår fra lokaler, som er beskyttet mod skader, forårsaget af fysiske forhold som f.eks. brand, vandskade, strømafbrydelse, tyveri eller hærværk.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
C.1	**Fysisk sikkerhedsafgrænsning** Procopa IT indhenter årligt erklæringer fra CibiCom og GlobalConnect, som dokumenterer at sikkerheden overholdes. Informationsaktiver i alle lokaler er beskyttet af fysisk adgangskontrol, og medarbejdere og eksterne parter har adgang via personlige adgangskort.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har observeret, at adgang til sikre områder er begrænset ved anvendelse af adgangssystem. Vi har ved inspektion gennemgået procedurer for fysisk sikkerhed vedrørende sikrede områder for at vurdere, om adgang til disse områder forudsætter dokumenteret ledelsesmæssig godkendelse, samt om personer uden godkendelse til sikrede områder skal registreres og ledsages af medarbejder med behørig godkendelse.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Styring af kommunikation og drift

Der er etableret:

- *passende forretningsgange og kontroller vedrørende drift, herunder monitorering, registrering og opfølgning på relevante hændelser*
- *tilstrækkelige procedurer for backup og beredskabsplaner*

passende funktionsadskillelse i og omkring it-funktionerne, herunder mellem udvikling, drift samt brugerfunktioner passende forretningsgange og kontroller vedrørende datakommunikationen, der på en hensigtsmæssig måde sikrer mod risiko for tab af autenticitet, integritet, tilgængelighed samt fortrolighed.

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
D.1	**Dokumenterede driftsprocedurer** Der forefindes drifts- og implementeringsprocedurer på alle væsentlige produktområder. Ansvaret for vedligeholdelse af disse ligger i de enkelte produktområder.	Vi har forespurgt ledelsen om, hvorvidt alle relevante driftsprocedurer er dokumenteret. I forbindelse med revision af de enkelte driftsområder er det ved inspektion kontrolleret, at der foreligger dokumenterede procedurer, samt at der er overensstemmelse mellem dokumentationen og de handlinger, som faktisk udføres. Vi har endvidere påset ved inspektion, at der foretages tilstrækkelig overvågning og opfølgning herpå.	Vores test har ikke ført til bemærkninger.
D.2	**Funktionsadskillelse** Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i it-afdelingen. Disse politikker og procedurer omfatter krav til, • at ansvar for udvikling og opdateringer til produktionsmiljøet er adskilte at it-afdelingen har ikke adgang til applikationer og transaktioner at udviklings- og driftsaktiviteter er adskilt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået brugere med administrative rettigheder til verificering af, at adgange er begrundet i et arbejdsbetinget behov og ikke kompromitterer funktionsadskillelse mellem udviklings- og produktionsmiljøer.	Vores test har ikke ført til bemærkninger.
D.3	**Foranstaltninger mod virus og lignende skadelig kode** Som en del af Azure services, sikres scanning af virus, derudover laver der halvårlig scanning i Azure for at sikre der ikke er skadelig kode i softwaren.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres.	Vores test har ikke ført til bemærkninger.
D.4	**Sikkerhedskopiering af informationer** Der bliver foretaget sikkerhedskopiering af data med passende mellemrum. Periodisk sker der test af, at data kan genskabes fra sikkerhedskopier.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået backupprocedurer samt påset, at de er tilstrækkelige og formelt dokumenteret. Vi har ved inspektion gennemgået log vedrørende backup til bekræftelse af, at backupper er gennemført fejlfrit, alternativt at der foretages afhjælpning i tilfælde af mislykkede backupper.	Vores test har ikke ført til bemærkninger.

D.5	**Monitorering af systemanvendelse og auditlogning** Der er implementeret logning ved adgang på kritiske systemer. Disse logge bliver gennemgået i tilfælde af mistanke om misbrug eller fejl. Procopa IT har ikke ansvaret for opsætning og drift af databaserne. Alle brugeres rettigheder bliver kontrolleret mindst én gang om året eller ved til-/afgang af medarbejdere. Alt hardware er overvåget. Der afsendes rapport i tilfælde af fejl. **Administrator- og operatørlog** Procopa IT logger transaktioner og handlinger, der er gennemført af brugere og administratorer via domain controllers (AD) audit log. Brugerkontis rettigheder på AD gennemgås periodisk. Logs fra AD og andre væsentlige systemer bliver gennemgået løbende og ved begrundet mistanke om uautoriserede handlinger.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, gennemgået systemopsætningen på services samt påset, at parametre for logning er opsat, således at handlinger, udført af brugere med udvidede rettigheder, bliver logget. Vi har ved inspektion påset, at der er etableret overvågning og alarmering for nedsat tilgængelighed samt for forsøg på brud på den etablerede sikringsforanstaltning Vi har endvidere ved inspektion kontrolleret, at der foretages tilstrækkelig opfølgning på logs fra kritiske systemer.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
E.1	**Brugerregistrering og administration af privilegier** Der er etableret processer for at sikre en korrekt tildeling af adgangsrettigheder til Procopa IT's data og it-systemer. Der udføres periodisk gennemgang af bruger- og adgangsrettigheder.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået procedurerne for brugeradministration samt kontrolleret, at kontrolaktiviteter er tilstrækkeligt dækkende. Vi har ved inspektion påset, at det er ledelsen, der godkender tildeling af adgang til systemerne, samt kontrolleret, at forretningsgangene er overholdt for oprettede brugere på Procopa IT's systemer. Vi har foretaget kontrol af, at årlige gennemgange foretages.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Adgangsstyring

Der er etableret:

- *passende forretningsgange og kontroller for tildeling af, opfølgning på samt vedligeholdelse af adgangsrettigheder til systemer og data*
- *logiske og fysiske adgangskontroller, som begrænser risikoen for uautoriseret adgang til systemer eller data fornødne logiske adgangskontroller, der underbygger den organisatoriske funktionsadskillelse.*

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
E.2	**Administration af brugeradgangskoder (password)** Interne- og driftsmiljøer kan tilgås Procopa ITs kontor eller via en sikker VPN-forbindelse. Brugerkonti til brug for adgang til VPN og Microsoft 365 er underlagt Multi Factor Authentication (MFA).	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres i forbindelse med passwordkontroller, og påset, at det sikres, at der anvendes passende autentifikation af brugere på alle adgangsveje. Vi har ved inspektion kontrolleret, at der anvendes en passende passwordkvalitet i Procopa IT's driftsmiljø – ved test af, at adgang til virksomhedens systemer sker ved brug af brugernavn og password.	Vores test har ikke ført til bemærkninger.
E.3	**Evaluering af brugeradgangsrettigheder** Ledelsen foretager periodisk gennemgang af brugerrettigheder til sikring af, at disse er i overensstemmelse med brugernes arbejdsbetingede behov. Uoverensstemmelser undersøges og udbedres rettidigt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har ved stikprøvevis inspektion kontrolleret, at der foretages periodiske gennemgange til bekræftelse af, at disse har fundet sted, samt påset, at identificerede afvigelser afhjælpes. Vi har endvidere stikprøvevis kontrolleret, at forretningsgangene er overholdt for oprettede brugere i Procopa IT's systemer.	Vores test har ikke ført til bemærkninger.
E.4	**Inddragelse af adgangsrettigheder** Brugerrettigheder til operativsystemer, netværk, databaser og datafiler vedrørende fratrådte medarbejdere bliver deaktiveret ved disses medarbejderes fratrædelse. Ledelsen godkender inddragelse af rettigheder og nedlæggelse af brugere.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at inddragelse af adgangsrettigheder sker efter betryggende forretningsgange, og at der foretages opfølgning i henhold til forretningsgangene på de tildelte adgangsrettigheder. Vi har endvidere ved stikprøvevis inspektion kontrolleret, at de beskrevne forretningsgange er overholdt for nedlagte brugere på systemer, samt at inaktive brugerkonti deaktiveres ved fratrædelse.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Udvikling og vedligeholdelse

- *Der er etableret passende forretningsgange og kontroller for implementering og vedligeholdelse*

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
F.1	**Styring af software på driftssystemer** Procopa IT har separate udviklings-, test- og produktionsmiljøer. It-miljøet for kundernes systemer er adskilt fra det interne it-miljø.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, for at adskillelse mellem enkelte miljøer opretholdes. Desuden har vi forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres for at opretholde kritiske systemer opdateret og gennemgået opdateringsprocedurernes tilstrækkelighed, hvad angår Procopa IT' egne væsentlige systemer samt kundernes systemer i henhold til kontraktlige aftaler. Vi har endvidere stikprøvevis efterprøvet kontrollerne, herunder at: • der er tilstrækkelig kommunikation med leverandørerne med henblik på at modtage nødvendige informationer om kritiske og vigtige opdateringer, samt at der foretages de fornødne risikovurderinger af de enkelte opdateringer. • de kritiske systemer er blevet opdateret hensigtsmæssigt.	Vores test har ikke ført til bemærkninger.
F.2	**Ændringsstyring** Procopa IT bruger change management til at styre ændringer. Ændringer af daglige arbejdsopgaver er beskrevet i standard change, som er forhåndsgodkendt.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres, og gennemgået change management-procedurernes tilstrækkelighed samt påset, at der er etableret et passende ændringshåndteringssystem, der er understøttet af en teknisk infrastruktur. Vi har ved stikprøvevis inspektion gennemgået ændringsønsker for følgende: • Registrering af ændringsanmodninger i det dertil etablerede system. • Dokumenteret test af ændringer, herunder godkendelse. • Godkendelse skal være opnået før implementering. Mundtlig ledelsesmæssig godkendelse anses for tilstrækkelig ved nødændringer, men skal dokumenteres efterfølgende. Dokumenteret plan for tilbagerulning, hvor relevant.	Vores test har ikke ført til bemærkninger.

Kontrolmål: Katastrofeplan

- *Procopa IT er i stand til at fortsætte servicering af kunder i en katastrofesituation.*

Nr.	Serviceleverandørens kontrolaktivitet	PwC's udførte testhandlinger	Resultat af test
G.1	**Opbygning/Struktur af katastrofeberedskab** Procopa IT har udarbejdet en katastrofeplan. Denne beskriver sandsynligheder samt de nødvendige tiltag. Planen er godkendt af ledelsen og revideres årligt. Katastrofeplanen tester Procopa IT's beredskab samt at vi overholder de dokumenterede krav nævnt i kontrakter.	Vi har forespurgt ledelsen om de procedurer/kontrolaktiviteter, der udføres. Vi har gennemgået udleveret materiale vedrørende katastrofeberedskab samt påset, at den organisatoriske og operationelle it-katastrofeplan indeholder ledelsesmæssige funktionsbeskrivelser, kontaktinformationer, varslingslister samt instrukser.	Vores test har ikke ført til bemærkninger.

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."

Daniel Lundbye
Kunde
Serienummer: CVR:34885486-RID:95494581
IP: 152.115.xxx.xxx
2023-03-21 07:33:07 UTC
NEM ID

Jesper Parsberg Madsen
Statsautoriseret revisor
Serienummer: d928e935-d26a-4251-b316-bc64d31db8a2
IP: 80.62.xxx.xxx
2023-03-21 07:36:59 UTC
MitID

Penneo dokumentnøgle: LUN14-F4SZF-XEL4E-2XCPS-AHJ62-BLCGC