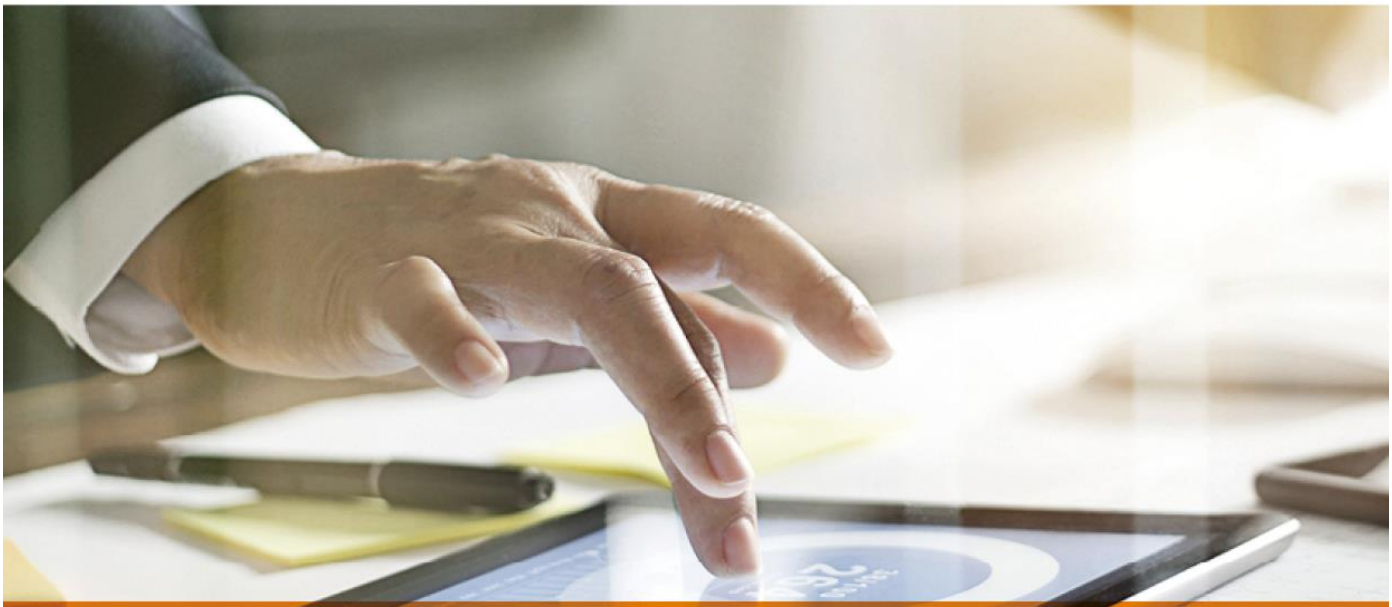
BEIERHOLM
VI SKABER BALANCE



PROCOPA IT

ISAE 3402 TYPE 2 ERKLÆRING

CVR: 34885486

Revisors erklæring vedrørende afdækning af de tekniske og organisatoriske sikringsforanstaltninger i tilknytning til hosting-aktiviteter i Procopa IT's hosting-miljø, som benyttes til private cloud-hosting for Procopa IT's kunder.

Beierholm
Godkendt Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet.

Kapitel 3:
Beskrivelse af kontrolmiljø.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf.

KAPITEL 1:

Ledelseserklæring

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt hosting-aktiviteter i Procopa IT´s hosting-miljø, 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, som er relevante for Procopa IT's kunders regnskaber.

Procopa IT anvender CibiCom og GlobalConnect som serviceunderleverandør for co-location. Erklæringen anvender partielmetoden og omfatter således 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 og fungerer effektivt sammen med vores kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten 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 hosting-miljø, der har behandlet kunders transaktioner i hele erklæringsperioden 1. januar 2024 til 31. december 2024. 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 hosting-miljø 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 hosting-miljøs 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) Indeholder relevante oplysninger om ændringer i generelle it-kontroller i relation til hosting-aktiviteter i Procopa IT´s hosting-miljø foretaget i erklæringsperioden

   (iii) 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 hosting-miljø, 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 hosting-miljø, 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 og fungerede effektivt i hele erklæringsperioden. 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,
(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele erklæringsperioden.

C. Der er etableret og opretholdt passende tekniske og organisatoriske sikringsforanstaltninger med henblik på at opfylde aftalerne med de dataansvarlige, god databehandlerskik og relevante krav til databehandler i henhold til databeskyttelsesforordningen.

Brøndby, d. 10. februar 2025

Daniel Lundbye, CEO

Procopa IT
Ringager 4E, 2605 Brøndby
CVR: 34 88 54 86

KAPITEL 2:

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

Til kunder af Procopa IT's hosting-serviceydelser 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 hosting-miljø, der har behandlet kunders transaktioner i erklæringsperioden fra 1. januar 2024 til 31. december 2024, og om udformningen og funktionen 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 og fungerede effektivt sammen med Procopa IT's kontroller. Erklæringen omfatter ikke hensigtsmæssigheden af udformningen og funktionaliteten af disse komplementære kontroller.

Procopa IT's ansvar

Procopa IT er ansvarlig for udarbejdelsen af kontrolbeskrivelsen i afsnit 3 samt tilhørende ledelseserklæring 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, implementeringen og effektivt fungerende kontroller for at opnå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om Procopa IT's beskrivelse samt om udformningen og funktionen 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 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 sine hosting-aktiviteter i Procopa IT´s hosting-miljø samt for kontrollernes udformning og funktionalitet. 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 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 opnået. 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 ledelseserklæringen.

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

Begrænsninger i kontroller hos Procopa IT

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 hosting-miljø, 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. 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 ledelseserklæringen. Det er vores opfattelse i forhold til erklæringsperioden 1. januar 2024 til 31. december 2024:

a) at beskrivelsen af de generelle it-kontroller i relation til hosting-aktiviteter i Procopa IT´s hosting-miljø, således som de var udformet og implementeret i hele erklærings-perioden 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 i hele erklæringsperioden, og
c) at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev opnået i alle væsentlige henseender, har fungeret effektivt i hele erklæringsperioden

Beskrivelse af testede 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 hosting-miljø, 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.

Søborg, d. 10. februar 2025

Beierholm
Godkendt Revisionspartnerselskab
CVR: 32 89 54 68

Kim Larsen
Statsautoriseret Revisor

Per Jensen
Senior Manager, IT-revision

KAPITEL 3:

Beskrivelse af kontrolmiljø

3.1 Introduktion

Beskrivelsen af generelle IT-kontroller vedrører hosting-aktiviteter i Procopa IT´s hosting-miljø, 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-location, fiber-kapaciteter og spamfilter.

3.2 Vision

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

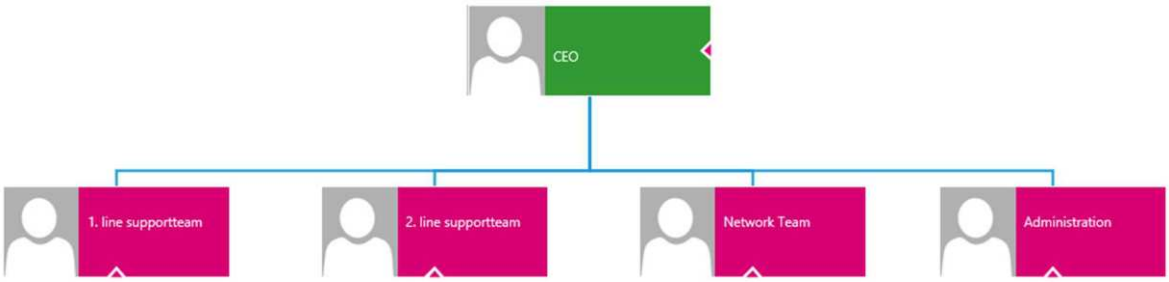
Procopa IT stiller en hosting-platform til rådighed, som kan sikre, at kunders data altid er i Danmark. Procopa IT arbejder ud fra en målsætning om at kunne være totalleverandør af infrastruktur, hosting og support med base i Danmark.

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 Ændringer i Procopa IT ApS i perioden

Procopa IT har ikke foretaget væsentlige ændringer i design eller udførelse af kontroller i erklæringsperioden.

3.5 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.

3.6 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 den 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.

3.6.1 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.

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

3.6.2 Eksterne parter

Procopa IT anvender kun leverandører godkendt af direktionen. Procopa IT anvender CibiCom og GlobalConnect som serviceunderleverandør for co-location.

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

Endvidere gennemføres en løbende inspektion af alle leverandører, der fungerer som databehandlere/underdatabehandlere for Procopa IT. Alle leverandører gennemgås løbende for at vurdere, om leverandørerne stadig leverer en relevant ydelse til Procopa IT.

3.7 Fysisk sikkerhed

Underleverandørerne GlobalConnect 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.

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

3.8 Styring af kommunikation og drift

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.

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

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.

3.8.1 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.

3.9 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 fra Procopa IT's kontor eller via en sikker VPN-forbindelse. Kundemiljøer kan kun tilgås via en VPN-forbindelse, som er beskyttet af MFA.

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

3.10 Udvikling og vedligeholdelse

Procopa IT har separate udviklings-, test- og produktionsmiljøer. It-miljøet for kundernes systemer er adskilt fra det interne it-miljø.

Procopa IT bruger change management til at styre ændringer. Ændringer af daglige arbejdsopgaver er beskrevet i standard change, som er forhåndsgodkendt.

3.11 Katastrofeplan

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.

3.12 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 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.

3.13 Kundernes ansvar

Procopa IT gør opmærksom på, at kunderne selv er ansvarlige for følgende kontroller:

- Kunderne skal selv foretage periodisk gennemgang af egne brugeres arbejdsbetinget behov for adgang til kundernes systemer og data. Procopa IT bistår med oprettelse, nedlæggelse og ændring af rettigheder.
- Kunderne skal selv sikre, at brugere overholder kundens egne politikker og procedurer, f.eks. passwordpolitik.

Procopa IT kan bistå med data og udtræk til disse kontroller.

KAPITEL 3:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultat heraf

Vi har struktureret vores arbejde i overensstemmelse med ISAE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør.

Vores test af kontrollernes design, implementering og funktionalitet har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af ledelsen og beskrevet i 4.2.

De udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design og implementering er foretaget ved metoderne beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Desuden vurderes det, om kontroller kan overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel til passende personale, som omfatter hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudførelse af kontrollen	Gentagelse af kontrollen med henblik på at verificere, om kontrollen fungerer som forudsat.

4.2 Kontrolmål, kontrolaktivitet, testhandlinger og konklusion

Kontrolmål A: Politik for informationssikkerhed
Ledelsen har udarbejdet en informationssikkerhedspolitik, der er rammesættende for organisatorisk ansvar samt udstikker klare, handlingsanvisende retningslinjer for it-sikkerhed for både medarbejdere og samarbejdspartnere.
Politikken revideres og ledelsesgodkendes mindst én gang årligt, og ved ændringer formidles disse til medarbejdere og samarbejdspartnere.

Serviceleverandørens kontrolaktivitet	Revisors test af kontroller	Resultat
Skriftlig informationssikkerheds-politik Der er en revideret og ledelsesgod-kendt skriftlig politik for informations-sikkerhed.	Vi har inspiceret politikken for informati-onssikkerhed, og det er påset, at politik-ken er revideret og ledelsesgodkendt i er-klæringsperioden.	Vi har ved vores test ikke konsta-teret afvigelser.
Ledelsesmæssigt og organisato-risk ansvar Politikken for informationssikkerhed fastslår det ledelsesmæssige og orga-nisatoriske ansvar.	Vi har inspiceret politikken for informati-onssikkerhed, og det er påset, at politik-ken forankrer ansvaret for informations-sikkerhed hos ledelsen. Vi har inspiceret politikken for informati-onssikkerhed, og det er påset, at politik-ken tydeliggør det organisatoriske omfang og ansvar.	Vi har ved vores test ikke konsta-teret afvigelser.
Formidling af informationssikker-hedspolitikken Det er ledelsens ansvar at sikre, at medarbejdere og samarbejdspartnere er bekendt med forventninger og krav specificeret i politikken for informati-onssikkerhed.	Vi har påset, at politikken for informati-onssikkerhed er tilgængelig for medarbej-dere på intranettet. Vi har inspiceret standard ansættelseskon-trakt for nye medarbejdere og påset, at der heri er krav om, at nye medarbejdere gør sig bekendt med politikken for infor-mationssikkerhed samt hvor den kan fin-des. Vi har inspiceret fortrolighedserklæringer for samarbejdspartnere og påset, at det er en fast del af kontrakten, at samarbejds-partneren orienteres om politikken for in-formationssikkerhed. Det er ved forespørgsel konstateret, at der har ikke været indholdsmæssige ændrin-ger til politikken for informationssikkerhed i erklæringsperioden.	Vi har ved vores test ikke konsta-teret afvigelser.

Kontrolmål B: Adgangsstyring til data og systemer
Ledelsen har sikret, at der er passende forretningsgange og kontroller for tildeling af arbejdsbetingede adgange og rettigheder til systemer og data. Hertil sikrer ledelsen opfølgning på tildelte rettigheder mindst en gang om året.
Til at understøtte adgangsstyringen er der implementeret krav til passwords samt behov for Multi-Factor Authentication (MFA). Derudover kan systemer og data kun tilgås fra internt netværk eller via VPN-forbindelse.

Serviceleverandørens kontrolaktivitet	Revisors test af kontroller	Resultat
Funktionsadskillelse og arbejdsbetinget behov Ledelsen har implementeret politikker og procedurer til sikring af tilfredsstillende funktionsadskillelse i it-afdelingen, og at adgange til systemer og data tildeles efter et arbejdsbetinget behov.	Vi har inspiceret politikken for informationssikkerhed, og det er påset, at der stilles krav til arbejdsbetinget behov ifm. brugeradgange. Vi har inspiceret procedurer og tjeklister for oprettelse og nedlæggelse af brugere. Vi er efter forespørgsel informeret om, at kunderne selv styrer, hvem der har adgang til deres data, og påset, at it-miljøerne er separate både ift. internt it-miljø samt ift. kundernes it-miljøer. Vi har påset organisatorisk opdeling ift. styring af rettigheder med 1., 2., og 3. line supportteam samt network team og administration/økonomi team.	Vi har ved vores test ikke konstateret afvigelser.
Adgangsbeskyttelse af systemer og data Det sikres, at brugere har unikke og personlige adgange til systemer og data, og at disse adgange tilføres yderligere beskyttelse via krav til adgangskoder, MFA, firewalls og VPN samt opdeling af interne og kunders it-miljøer.	Vi har inspiceret politikken for informationssikkerhed og påset, at den indeholder krav til kompleksiteten af passwords Vi har inspiceret politikken for informationssikkerhed og påset, at den indeholder krav netværkssikkerhed samt regler og godkendelse vedrørende oprettelse af nye netværk. Vi har observeret, at der er tilfredsstillende og korrekt implementering af Multi-Factor Authentication (MFA) samt Virtual Private Network (VPN) for adgang til data og systemer.	Vi har ved vores test ikke konstateret afvigelser.

Gennemgang og evaluering af adgange Ledelsen sikrer gennemgang og evaluering af brugeradgange og rettigheder mindst en gang årligt samt at der er en procedure, der sikrer, at adgange og rettigheder nedlægges, når en medarbejder forlader virksomheden.	Vi har inspiceret politikken for informationssikkerhed og påset, at den indeholder krav om nedlæggelse af adgange og brugerrettigheder, når brugeren ikke længere har behov for adgang. Vi har inspiceret procedurer og tjeklister for oprettelse og nedlæggelse af brugere.	Vi har ved vores test ikke konstateret afvigelser.

Kontrolmål C: Adgangsstyring fysiske lokationer
Ledelsen har sikret, at der er passende sikkerhedsmæssige foranstaltninger til den fysiske adgang til virksomheden. Derudover sikrer ledelsen, at leverandører lever op til passende sikkerhedsmæssige foranstaltninger, således driftsafvikling foregår fra lokationer, der er beskyttet mod uautoriseret adgang samt skader forsaget af fysiske forhold.

Serviceleverandørens kontrolaktivitet	Revisors test af kontroller	Resultat
Fysisk adgangskontrol til eget kontormiljø Der er implementeret fysisk adgangskontrol med unikt, personligt adgangskort, således det logges, hvem der låser sig ind til virksomhedens kontormiljø.	Vi har påset, at alle medarbejdere har egen, unik medarbejdernøgle med adgang til virksomhedens kontormiljø.	Vi har ved vores test ikke konstateret afvigelser.
Fysisk adgangskontrol til datacentre Det sikres, at kun medarbejdere med arbejdsbetinget behov herfor har adgang til leverandørernes datacentre.	Vi har påset, at kun udvalgte medarbejdere med et arbejdsbetinget behov har adgang til leverandørernes datacentre.	Vi har ved vores test ikke konstateret afvigelser.
Sikring af leverandørernes datacentre Det sikres, at leverandører lever op til passende sikkerhedsmæssige foranstaltninger af deres datacentre ved at indhente og gennemgå de relevante ISAE 3402-erklæringer.	Vi har påset, at der er indhentet og gennemgået ISAE3402-erklæringer fra Cibicom A/S og GlobalConnect A/S i erklæringsperioden.	Vi har ved vores test ikke konstateret afvigelser.

Kontrolmål D: Drift og ændringsstyring
Ledelsen har sikret, at der er udarbejdet passende handlingsanvisende procedurer til styring af den daglige drift, herunder sikring af sagshåndtering og ændringsstyring.

Serviceleverandørens kontrolaktivitet	Revisors test af kontroller	Resultat
Procedurer for driftsrelaterede opgaver Der er udarbejdet procedurer, der er relevante for den daglige drift af løsninger til kunderne, som er handlingsanvisende og lettilgængelige for medarbejderne.	Vi har forespurgt ledelsen samt medarbejder ift. de mest anvendte procedurer. Vi har påset, at disse er let tilgængelige og handlingsanvisende samt at der er anvist en ansvarlig for sikring af revidering og korrekthed af disse.	Vi har ved vores test ikke konstateret afvigelser.
Sagshåndtering Der er implementeret passende procedure for sagshåndtering, således henvendelser fra kunder håndteres rettidigt, struktureret og dialogbaseret.	Vi har inspiceret procedure for sagshåndtering og påset, at den er revideret i erklæringsperioden samt handlings- og procesanvisende for kundehenvendelser.	Vi har ved vores test ikke konstateret afvigelser.
Ændringsstyring Der er implementeret passende procedurer for change management til at håndtere ændringsønsker. Herunder handlinger forbundet med risikovurdering samt konkrete handlinger forbundet med tilbagerulning af ændringer.	Vi har inspiceret procedure for ændringsstyring (request for change - RFC) og påset, at denne er tilstrækkelig og handlingsanvisende. Vi har inspiceret standardformularen for RFC samt konkrete eksempler på RFC-sager og påset, at der er korrekte krav om og udfyldelse af: - Beskrivelse for baggrund for ønsket - Beskrivelse af ønsket - Beskrivelse af rollback, såfremt RFC medfører fejl - Påvirkning af RFC - Risikovurdering - Ledelsesgodkendelse.	Vi har ved vores test ikke konstateret afvigelser.
Styring af software på driftssystemer Der er implementeret passende procedurer for at sikre rettidig opdatering af systemer og software til nyeste versioner med så lav impact på driften som muligt.	Vi har forespurgt ledelsen om procedurer og kommunikation med kunder ifm. opdatering af systemer. Vi har inspiceret procedure for opsætning af automatisk opdatering af servere. Vi har inspiceret sagshåndtering og korrespondancer og påset, at der er rettidig kommunikation ifm. Systemopdateringer og -ændringer.	Vi har ved vores test ikke konstateret afvigelser.

Kontrolmål E: Sikring af data
Der er implementeret passende procedurer og foranstaltninger til at sikre data samt sikring af procedurer for at handle og at genskabe data i tilfælde af hændelser, der påvirker dataintegriteten.

Serviceleverandørens kontrolaktivitet	Revisors test af kontroller	Resultat
Backup af data Der er implementeret procedure for backup af data.	Vi har inspiceret procedurer for backup af data samt påset en rutinemæssig backup via backup-rapportering.	Vi har ved vores test ikke konstateret afvigelser.
Gendannelse af data Der er implementeret passende procedure for gendannelse af data, herunder årlig test af genskabelse.	Vi har inspiceret IT-beredskabsplanen og påset, at der er krav om årlig restoretest. Herunder er det påset, at den årlige test er gennemført tilfredsstillende.	Vi har ved vores test ikke konstateret afvigelser.
Hændelseshåndtering og beredskab Der er implementeret passende procedurer til at håndtere hændelser eller risiko for hændelser, der påvirker dataintegriteten. Herunder en IT-beredskabsplan, der anviser ansvar samt handlinger i prioriteret rækkefølge.	Vi har inspiceret politikken for informationssikkerhed og påset, at der er handlingsanvisning til medarbejdere, der opdager trusler mod, eller direkte brud på, informationssikkerheden. Vi har inspiceret IT-beredskabsplanen og påset, at denne er revideret i erklæringsperioden. Vi har inspiceret IT-beredskabsplanen og påset, at denne indeholder: - Kontaktpersoner og leverandører - Strategi for kommunikation - Forskellige hændelser med tilpassede handlinger - Krav om årlig test af restore. Vi har påset, at virksomheden udarbejder hændelsesrapporter, der påviser: - Fejlbeskrivelse - Hvorfor fejlen opstår - Hvordan fejlen er udbedret - Hvordan man sikrer sig mod gentagelser.	Vi har ved vores test ikke konstateret afvigelser.

Virus-, malware- og kode-beskyttelse Der er sikring mod vira og malware på virksomhedens enheden, herunder sikring af installation og opdatering til nyeste versioner.	Vi har forespurgt ledelsen, hvordan man sikrer enheder og miljøer mod skadelig kode. Det er påset, at der føres tilsyn med end-point compliance ift. beskyttelse mod virus og malware. Ydermere er det oplyst, at der, som en del af Azure Services, sikres scanning for virus samt halvårlig scanning, der søger efter skadelig kode i software. Det er observeret, at der scannes for virus og malware samt påset, at der ikke findes non-compliant end point-udstyr i it-miljø.	Vi har ved vores test ikke konstateret afvigelser.
Monitorering og logning af systemer og data Der pågår monitorering af systemerne og data samt logning af medarbejdernes tilgang hertil, således det er muligt at gennemgå logs ved bekrundet mistanke om eller ved konstatering af uautoriserede handlinger.	Vi har forespurgt ledelsen om de kontrolaktiviteter, der udføres ifm. monitorering og logning samt hvorledes der følges op på uregelmæssigheder. Kontrolaktiviteter samt opfølgning vurderes passende. Vi har påset, at der foregår monitorering af systemerne samt logning af medarbejderadgang samt observeret at der fremsendes rapport i tilfælde af fejl.	Vi har ved vores test ikke konstateret afvigelser.
Kryptering af data Data, både intern og kunders, sikres passende kryptering efter en klassifikation af data.	Vi har inspiceret politikken for informationssikkerhed og påset, at der er krav om klassificering af data i en af deangivne kategorier samt krav om dertil passende kryptering.	Vi har ved vores test ikke konstateret afvigelser.

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

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

Per Højbjerg Jensen
Beierholm Godkendt Revisionspartnerselskab CVR: 32895468
Senior Manager
På vegne af: Beierholm
Serienummer: 06e264f6-b561-4135-b34d-b5d3f080562c
IP: 212.98.xxx.xxx
2025-02-10 12:22:41 UTC

Kim Holm Larsen
Beierholm Godkendt Revisionspartnerselskab CVR: 32895468
Statsautoriseret Revisor
På vegne af: Beierholm Godkendt Revisionspartnersels…
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2025-02-10 12:24:24 UTC

Daniel Lundbye
PROCOPA IT ApS CVR: 34885486
CEO
På vegne af: Procopa IT
Serienummer: 69ec243a-3312-4c14-ab0c-8dd7011760e3
IP: 87.49.xxx.xxx
2025-02-10 12:37:09 UTC