AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED PR. 13 MARTS 2025 OM BESKRIVELSEN AF DRIFTS- OG HOSTING-YDELSER OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING

SAC-IT A/S

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED PR. 13 MARTS 2025 OM BESKRIVELSEN AF DRIFTS- OG HOSTING-YDELSER OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING

Til: Ledelsen i SAC-IT A/S
SAC-IT A/S' kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om den af SAC-IT A/S (serviceleverandøren) pr. 13 marts 2025 udarbejdede beskrivelse i sektion 3 af drifts- og hosting-ydelser og de tilhørende kontroller, og om udformningen af de indførte kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

Serviceleverandørens ansvar

Serviceleverandøren er ansvarlig for udarbejdelse af udtalelsen i sektion 2 og den medfølgende beskrivelse, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå udtalelsen og beskrivelsen er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom serviceleverandøren er ansvarlig for at anføre kontrolmålene samt udforme og implementere 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.

BDO Statsautoriseret revisionsaktieselskab 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 serviceleverandørens beskrivelse samt om udformningen af kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed om kontroller hos en serviceleverandør. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt 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 samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte kontrolmål og hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i sektion 2.

Som nævnt ovenfor har vi ikke udført handlinger vedrørende den operationelle effektivitet af de kontroller, der indgår i beskrivelsen, 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

Serviceleverandørens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af virksomhedens kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved anvendelsen af drifts- og hosting-ydelser, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør som følge af deres art muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner.

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 serviceleverandørens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af drifts- og hosting-ydelser og de tilhørende kontroller, således som de var udformet, og implementeret pr. 13 marts 2025, i alle væsentlige henseender er retvisende, og

b. at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 13 marts 2025.

Beskrivelse af test af kontroller

De specifikke kontroller, der blev testet, og resultater af disse tests fremgår i sektion 4.

Tiltænkte brugere og formål

Denne erklæring er udelukkende tiltænkt kunder, der har anvendt serviceleverandørens drifts- og hosting-ydelser, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kundens egne kontroller, ved opnåelsen af en forståelse af kundernes informationssystemer, der er relevante for regnskabsaflæggelsen.

København, den 19. marts 2025

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

Mikkel Jon Larssen
Partner, Lead of Risk Assurance, CISA, CRISC

2. SAC-IT A/S' UDTALELSE

SAC-IT A/S udfører drifts- og hostning-ydelser som leveres til serviceleverandørens kunder.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt drifts- og hosting-ydelser, 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, når de opnår en forståelse af kunders informationssystemer, som er relevante for regnskabsaflæggelsen.

SAC-IT anvender serviceunderleverandører. Disse serviceunderleverandørens relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

SAC-IT A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af drifts- og hosting-ydelser og de tilhørende kontroller pr. 13 marts 2025. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for drifts- og hosting-ydelser, og hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:

    - De typer af ydelser, der er leveret, herunder behandlede grupper af transaktioner, 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.
    - Hvordan systemet behandlede andre betydelige begivenheder og forhold end transaktioner.
    - Processen, der blev anvendt til at udarbejde rapporter 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 brugervirksomhederne, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå.
    - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for behandlingen og rapporteringen af kunders transaktioner

2. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af drifts- og hosting-ydelser og de tilhørende kontroller under hensyntagen til, at denne beskrivelse 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 drifts- og hosting-ydelser, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

SAC-IT A/S bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 13 marts 2025. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. 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.

Vedbæk, den 19. marts 2025

SAC-IT

Jackie Amelung
CEO

3. SAC-IT A/S BESKRIVELSE AF IT-KONTROLLER VEDRØRENDE REGNSKABS AFLÆGGELSEN FOR SAC-IT'S SERVICES.

3.1 GENERAL BESKRIVELSE AF SAC-IT A/S

SAC-IT er en danskejet virksomhed som leverer Cloud-, Hosting- og Datacenter-services, som bygges med udgangspunkt i den enkelte kundes behov. Vi leverer vores services til både den private og offentlige sektor. SAC-IT har kontorer i Vedbæk og Fredericia. Ejerkredsen udgør Jens Morten Hansen, Jackie Amelung og Jakob Arndt.

SAC-IT' ca. 30 medarbejdere er specialiserede inden for VMware, serverdrift, support og informationssikkerhed, og organiseret i en cloudafdeling, drift- og supportafdeling, økonomiafdeling, salg/marketing compliance & securityafdeling, og en administrationsafdeling.

I forbindelse med udførelsen af vores service kan det være nødvendigt at gøre brug af ekstern assistance. Vi sikrer os altid, at aftaler med eksterne serviceleverandører og outsourcing leverandører er formaliseret, hvor det er relevant, og at samarbejdspartnere er bekendt med vores it-sikkerhedspolitik samt underskriver fortrolighedserklæring efter behov.

3.2 SERVICES

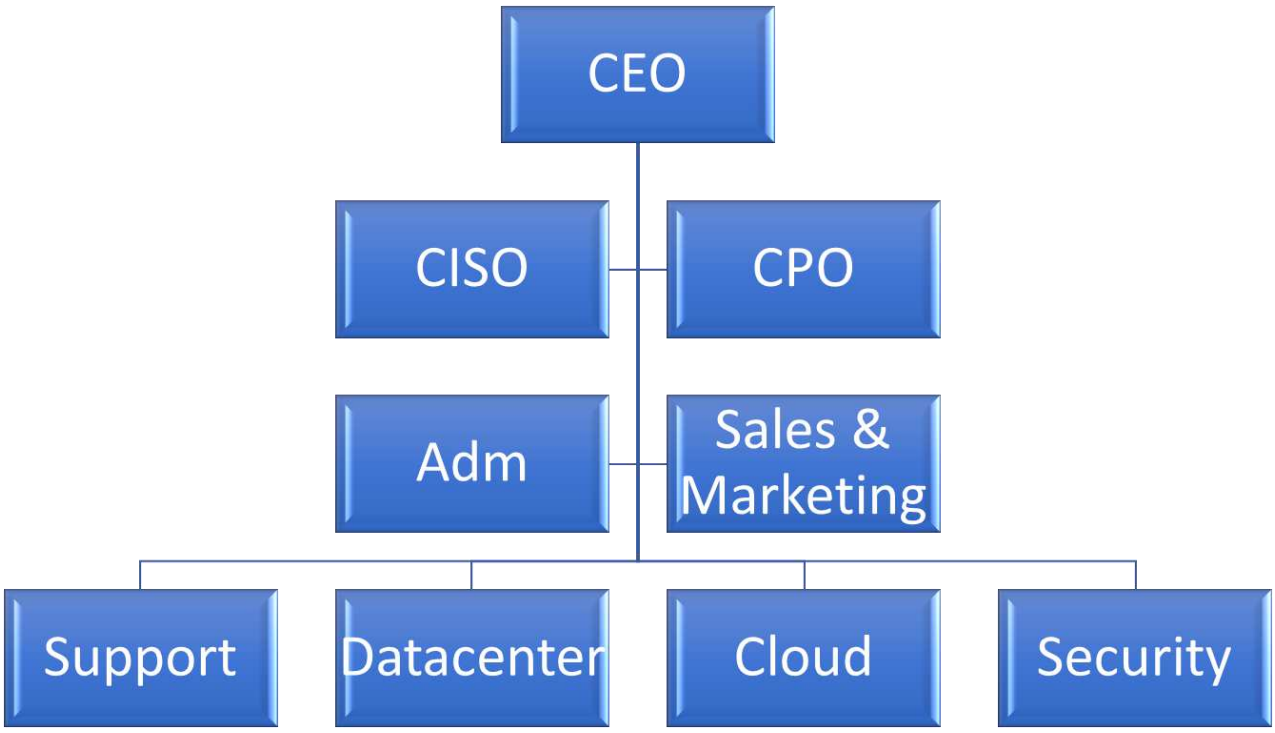
Kundeservices

- Managed services (it-outsourcing og hosting/housing)
- Servicedesk & support
- Drift og driftsadministration
- Cloud baserede løsninger (modern workplace, baseline security tools)
- Security & compliance
- Fjernbackup
- Rådgivning (it-sikkerhed og compliance)

Interne servicefunktioner

- Intern IT (cloud og anden server/netværk infrastruktur)
- Finance
- Human ressource
- Salg og marketing
- Compliance & security
- Projektledelse

3.3 SAC-IT' ORGANISATION



3.4 RISIKOVURDERING

SAC-IT A/S laver årligt en risikovurdering, der omfatter it-installationerne og brugen heraf iforb. med revisionserklæringen. Der arbejdes dog kontinuerligt med sikkerhed og risikovurdering indenfor alle services og afdelinger. Der tages udgangspunkt i det nuværende trusselbillede, og risikovurderingen er en del af dokumentationen til den årlige it-revision. På baggrund at revisionens anbefalinger kan denne danne grundlag for nye projekter, der skal styrke informationssikkerheden på alle SAC-IT A/S it-platforme.

Denne rapport omfatter udelukkende kontrol- og kontrolmål for processer og kontroller, der styres af SAC-IT A/S, og den omfatter således ikke kontroller eller kontrolmål, der styres af underleverandører.

3.5 KONTROLRAMME, KONTROLSTRUKTUR OG KRITERIER FOR KONTROL IMPLEMENTERING

SAC-IT A/S informationssikkerhed er defineret ud fra målsætningen om at levere dedikeret it-outsourcing og infrastrukturløsninger af høj kvalitet, herunder stabilitet og sikkerhed.

Kontrollerne er bakket op af SAC-ITs sikkerhedspolitik. Denne politik revideres løbende og håndteres via samme proces som kontrollerne i SAC-IT' ISMS. Kontrolmiljøet faciliteres af CISO i tæt dialog med ledelsen.

Fastlæggelsen af kriterier og omfang af kontrolimplementering hos SAC-IT A/S er baseret på ISO 27002:2022-rammen for styring af informationssikkerhed. Følgende kontrolområder i ISO 27002 blev vurderet:

- A.5 Organisatoriske foranstaltninger
- A.6 Personrelaterede foranstaltninger
- A.7 Fysiske foranstaltninger
- A.8 Teknologiske foranstaltninger

Implementeret kontrolmiljø
De implementerede kontroller er baseret på de ydelser, som SAC-IT A/S leverer til kunder og omfatter kontrolområder og kontrolaktiviteter. Alle ovenstående områder er beskrevet detaljeret i det følgende i separate afsnit, og de beskrevne kontrolmål og kontroller for disse områder i afsnittet om kontrolmål, kontroller, test og resultat af test er en integreret del af beskrivelsen.

A.5: Organisatoriske foranstaltninger

A.5.1 Politikker for informationssikkerhed
SAC-IT A/S har indført politikker og procedurer, der sikrer, at SAC-IT A/S har passende tekniske og organisatoriske sikkerhedsforanstaltninger. SAC-IT har udarbejdet og implementeret en af ledelsen godkendt informationssikkerhedspolitik, der løbende gennemgås og opdateres.

A.5.2 Roller og ansvar for informationssikkerhed
SAC-IT A/S har implementeret kontroller for at sikre en generel styring af informationssikkerheden, herunder uddelegering af ansvar og håndtering af væsentlige risici i overensstemmelse med kravene fra virksomhedens ledelse.

SAC-IT A/S sikrer, at samme person ikke har adgang til at tilgå, ændre og anvende systemer, informationer eller infrastruktur, uden at dette er godkendt eller vil blive opdaget.

A.5.3Funktionsadskillelse
SAC-IT A/S funktioner og ansvarsområder er adskilt, i det omfang det er muligt taget virksomhedens størrelse i betragtning, for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af data.

A.5.4 Ledelsens ansvar
Ledelsen tager aktivt del i it-sikkerheden i organisationen. Det formelle ansvar, herunder godkendelse af informationssikkerhedspolitikken, påhviler også den administrerende direktør.

A.5.9 Fortegnelse over information og understøttende aktiver
SAC-IT A/S vedligeholder en fortegnelse over aktiver der anvendes til levering af services herunder de ansattes udstyr. Alle aktiver er tildelt en ejer.

A.5.15 Administration af adgang
SAC-IT A/S har implementeret kontroller for at sikre, at adgang til systemer, data og netværkstjenester gives gennem en dokumenteret proces i overensstemmelse med et relevant arbejdsrelateret behov og lukkes ned, når den relevante adgang ikke længere er nødvendig.

A.5.16 Styring af identifikation
SAC-IT A/S har opstillet en procedure for registrering og afmelding af bruger i forbindelse med tildeling af adgangsrettigheder.

A.5.17 Autentifikationsoplysninger
SAC-IT A/S har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. Udformning af krav til blandt andet længde, kompleksitet, løbende udskiftning og historik af password samt lukning af brugerkonto efter forgæves adgangsforsøg følger best practise for en sikker logisk adgangskontrol. Der er udformet tekniske foranstaltninger, der understøtter disse krav. Når arbejdsstationer forlades, er der sikret anvendelse af skærmlås. Krav om anvendelse af skærmlås er beskrevet i it-sikkerheds-politikken.

A.5.18 Adgangsrettigheder
SAC-IT A/S har opstillet en procedure for adgangsstyring af tildeling og tilbagekalde af adgangsrettigheder.

Alle adgange og rettigheder gennemgås med jævne mellemrum af SAC-IT A/S.

SAC-IT A/S har en procedure for, at ved ophør eller medfratrædelse, så inddrages og tilpasses adgangsret-tigheder.

A.5.19 Informationssikkerhed i leverandørforhold
SAC-IT A/S bruger adskillige underleverandører af backup.
Der bliver løbende ført tilsyn med nedenstående leverandører jvfr. SAC-IT-procedure for tilsyn.

- Veeam
- Avepoint
- N-able Cove
- Awamar

SAC-IT A/S bruger Digital Realty (InterXion) og Fuzion som underleverandør af datacenter infrastruktur.
De står begge for den fysiske sikkerhed og adgange.

Tjenesten leveret af InterXion og Fuzion inkluderer:
- Overvågning af de fysiske placeringer
- Vagtservice i tilfælde af alarm
- ID-kort
- Iris scanning i sluse

SAC-IT A/S har fastsat informationssikkerhedskrav til anvendte underleverandører.

SAC-IT A/S har begrænset underleverandørers adgang til relevante systemer og data i forhold til underleve-randørens arbejdsbetingede behov.

A.5.20 Håndtering af informationssikkerhed i leverandørforhold
SAC-IT A/S har fastsat informationssikkerhedskrav til anvendte underleverandører i indgået serviceaftale.

A.5.22 Overvågning, vurdering og ændringsstyring af leverandørydelser
SAC-IT A/S udfører årligt tilsyn med anvendte underleverandører, herunder indhenter og gennemgår under-serviceleverandørens revisorerklæringer, certificeringer og lignende. Tilsyn af underserviceleverandører fore-tages minimum en gang om året og er baseret på en risikovurdering.

Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents
SAC-IT A/S har implementeret procedure for håndtering af brud på informationssikkerheden herunder fordelt roller og ansvar i forbindelse med brud på informationssikkerheden.

Dokumenterede driftsprocedurer
SAC-IT A/S har indført driftsprocedurer, der sikrer, sikker drift af informationsbehandlingsfaciliteter. Driftsprocedurer gjort tilgængelige for relevante ansatte.

A.6: Personrelaterede foranstaltninger

A.6.1 Screening
Før ansættelse af medarbejdere gennemføres der tilstrækkelig screening af potentielle ansøgere herunder indhentelse af straffeattest.

A.6.3 Awareness, uddannelse og træning vedrørende informationssikkerhed
Nye medarbejdere modtager tilstrækkelig information i informationssikkerhed ved ansættelse herunder underskriver informationssikkerhedspolitikken

SAC-IT A/S foretager løbende, og minimum én gang årligt, awareness træning i henhold til informationssikkerhed samt håndteringen heraf.

A.6.7 Distancearbejde
SAC-IT A/S har indført procedurer, der sikrer, at adgang fra arbejdspladser uden for SAC-IT A/S lokaler og fjernadgang til systemer og data sker via krypterede forbindelser, samt at alle mobile enheder har installeret antivirus software, der opdateres løbende. Alt fjernadgang skal foregå via to-faktor autentifikation.

A.6.8 Indrapportering af informationssikkerhedshændelser
SAC-IT A/S har indført procedurer, der sikrer at eventuelle informationssikkerhedshændelser og informationssikkerhedssvagheder rapporteres til relevante parter.

A.7: Fysiske foranstaltninger

A.7.1 Fysisk områdesikring
SAC-IT A/S har implementeret procedurer kontroller for at sikre, at it-udstyr er ordentligt beskyttet mod uautoriseret fysisk adgang og miljøhændelser

A.7.2 Fysisk adgangskontrol
SAC-IT A/S lokaler har adgangskontrol i form af en påkrævet personlig kode og en systemnøgle for at sikre, at kun autoriseret personale har adgang. Kun SAC-IT A/S medarbejdere modtager en nøgle og en kode. Hvis leverandører, konsulenter eller andre eksterne parter skal have adgang, er dette kun muligt sammen med autoriseret personale.

A.7.5 Beskyttelse mod fysiske og miljømæssige trusler
SAC-IT A/S sikrer, at udstyr beskyttes mod fysiske og miljømæssige trusler, herunder at specificerede krav til serverrum overholdes.

A.7.8 Placering og beskyttelse af udstyr
Det kritiske udstyr placeres i serverrummet, hvortil kun teknisk personale og SAC-IT A/S partnere har adgang.

A.7.11 Forsyningssikkerhed
SAC-IT A/S har implementeret procedurer for at sikre, at udstyr beskyttet mod strømafbrydelser mv., samt at alle databærende kabler er beskyttet.

A.7.13 Vedligeholdelse af udstyr
SAC-IT A/S sikrer, at alt vedligeholdelse af udstyr kun udføres af autoriseret personale og sker i overensstemmelse med den gældende vedligeholdelsesplan.

A.8: Teknologiske foranstaltninger

A.8.2 Privilegerede adgangsrettigheder
Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres. Privilegerede adgangsrettigheder tildeles derfor udelukkende ud fra et arbejdsbetinget behov.

A.8.3 Begrænset adgang til information
For at forhindre uautoriseret adgang til informationer og understøttende aktiver, skal adgange begrænses mest muligt i overensstemmelse med SAC-IT A/S politik for adgangsstyring.

A.8.5 Sikker autentifikation
SAC-IT A/S har implementeret procedurer og foranstaltninger for at sikre at brugere autentificeres på sikker vis, når der gives adgang til systemer, applikationer og tjenester.

A.8.7 Beskyttelse mod malware
Alle registrerede servere i SAC-IT A/S infrastruktur er opdateret med godkendt antivirussoftware i henhold til Best Practice inden for området. Når en ny server er sat op, sikrer arbejdsgange i SAC-IT A/S servicedesk, at antivirus er installeret.

Alle arbejdsstationer i SAC-IT A/S er opdateret i henhold til Best Practice med antivirussoftware. Nye arbejdsstationer installeres med et standardbillede, som indeholder antivirus.

A.8.8 Styring af tekniske sårbarheder
SAC-IT A/S indhenter løbende information om tekniske sårbarheder, som efterfølgende evalueres og håndteres ved passende tiltag.

A.8.9 Konfigurationsstyring
SAC-IT A/S har implementeret procedurer og værktøjer til at håndhæve og styre de definerede konfigurationer i forhold til sikkerhedsindstillinger for hardware, software, tjenester og netværk.

A.8.13 Backup af information
Der tages backup af alle vigtige data i henhold til kundeaftaler. Fejl i backup identificeres af backupværktøjet og registreres i SAC-IT A/S servicedesk. Gendannelsestest for kunden udføres kun, når der eksisterer en specifik aftale mellem kunden og SAC-IT A/S.

A.8.15 Logning
Brugertransaktioner herunder succesfulde og mislykkede adgangsforsøg, undtagelser og sikkerhedshændelser logges, og loggen gemmes i henhold til de opbevaringsperioder, der er aftalt med kunden.

SAC-IT A/S har implementeret interne procedurer for at sikre, at alarmer adresseres for at reagere på relevante hændelser og handle derefter. Alle relevante alarmer vises på storskærm inden for normal arbejdstid og til vagthavende i vagtperioder. Alle alarmer gennemgås dagligt af SAC-IT A/S driftsafdeling og rapporteres til kunder, fordi sager oprettes på baggrund heraf.

Alle hændelser registreres i SAC-IT A/S IT Service Management System.

Systemadministratorers handlinger logges automatisk i vores servicedesk system.

Der er opsat overvågning med henblik på fremtidig analyse af fejl og hændelser i vores servicedesk.

A.8.18 Brug af privilegerede understøttende programmer
For at undgå skade på systemet, begrænses brugen af understøttende programmer, så kun autoriserede medarbejdere kan anvende disse.

A.8.19 Softwareinstallation i test- og produktionssystemer
SAC-IT A/S har implementeret procedurer og tiltag til sikker styring af softwareinstallationer i test- og produktionssystemer. Herunder sikre integritet af test- og produktionssystemer og forhindre udnyttelse af tekniske sårbarheder.

SAC-IT A/S har desuden opstillet generelle krav for installation af software på arbejdsstationer og servere.

A.8.20 Netværkssikkerhed
SAC-IT A/S har implementeret kontroller for at sikre, at driften af materielle infrastrukturkomponenter udføres på en struktureret og sikker måde.

SAC-IT A/S har skriftlige procedurer for konfiguration af firewalls, routere og switches, som udelukkende udføres af driftsafdelingen.

A.8.21 Sikring af netværkstjenester
Adgang til hosting infrastruktur for vores kunder går enten gennem offentlige netværk, hvor adgangen sker via krypteret fjernadgang og firewall. Adgang og kommunikation mellem vores servere og internettet går gennem vores centralt styrede firewall, hvor der er opsat logning. Al indkommende netværkstrafik går gennem vores firewalls. Kun godkendt netværkstrafik er tilladt gennem firewallen baseret på en kundeanmodning.

A.8 22 Segmentering af netværk
Kundenetværk er begrænset af VLAN- og adgangsreglerne i vores Core-router/firewall.

A.8.32 Ændringsstyring
SAC-IT A/S har en formel procedure for ændringsstyring for at sikre, at systemerne revurderes og testes i forbindelse med større ændringer og følger processen i vores servicedesk system i form af formaliserede arbejdsgange. Sikkerhedsrettelser laves en gang om måneden i de servicevinduer, der er aftalt med kunderne. Alle andre service packs installeres udelukkende efter ønske og følger processen i vores servicedesksystem i form af formaliserede arbejdsgange.

KOMPLEMENTERENDE KONTROLLER HOS SERVICELEVERANDØREN

Kunden er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene og dermed i overensstemmelse med relevant lovgivning:

- Kunden har ansvaret for at sikre, at administratorernes brug af drifts- og hosting-ydelser og den behandling af data, der foretages i systemet, sker i overensstemmelse med relevant lovgivning.
- Kunden kontrollerer brugerrettighederne i drifts- og hosting-ydelser, herunder hvilke personer der tildeles administratoradgang, og hvilke rettigheder de enkelte administratorer tildeles.
- Kunden har til ansvar for at der foretages restore test af kundens sikkerhedskopiering

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST

Formål og omfang

BDO har udført sit arbejde i overensstemmelse med ISAE 3402 om erklæringsopgaver med sikkerhed om kontroller hos en serviceorganisation.

BDO har udført handlinger for at opnå bevis for oplysningerne i SAC-IT A/S' beskrivelse af drifts- og hosting-ydelser samt for udformningen af de tilhørende kontroller. De valgte handlinger afhænger af BDO's vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet.

BDO's test af udformningen af kontroller samt implementeringen heraf har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af SAC-IT A/S, og som fremgår af efterfølgende kontrolskema.

I kontrolskemaet har BDO beskrevet de udførte test, der blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og at de tilhørende kontroller var hensigtsmæssigt udformet pr. 13 marts 2025.

Udførte testhandlinger

Test af udformningen af kontroller samt implementeringen heraf er udført ved forespørgsel, inspektion og observation.

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.

For de ydelser, som Fuzion leverer inden for hosting, har vi modtaget en ISAE 3402 gældende fra den 1. juni 2023 til den 28. februar.2025 vedrørende serviceunderleverandørens kontroller.

For de ydelser, som InterXion leverer inden for hosting, har vi modtaget en SOC 2 erklæring gældende fra den 1. januar 2023 til den 31. december 2023 vedrørende serviceunderleverandørens kontroller.

Disse serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i SAC-IT' beskrivelse af drifts- og hosting-ydelser og de tilhørende kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos SAC-IT, der sikrer overvågning af serviceunderleverandørens opfyldelse af den mellem serviceunderleverandøren og SAC-IT indgåede aftale.

Resultat af test

Resultatet af de udførte test af kontroller angiver, om den beskrevne test har givet anledning til at konstatere afvigelser.

En afvigelse foreligger, når:

- Kontroller mangler at blive udformet og implementeret for at kunne opfylde et kontrolmål.
- Kontroller, der knytter sig til et kontrolmål, ikke er hensigtsmæssigt udformet eller implementeret.

Risikovurdering			
Kontrolmål	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
Risikovurdering At sikre, at serviceleverandøren udfører en årlig risikovurdering i forhold til grundlaget for de tekniske og organisatoriske sikkerhedsforanstaltninger.	▶ Der foretages løbende og som minimum en gang årligt en risikovurdering af drifts- og hosting-ydelser baseret på potentielle risici for datas tilgængelighed og fortrolighed. ▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler. ▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. ▶ Risikovurderinger opdateres løbende efter behov, men minimum en gang årligt.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedurer for IT-risikostyring og observeret, at proceduren er udarbejdet og implementeret inden erklæringsdatoen. Vi har inspiceret serviceleverandørens risikoregister og observeret, at risici er vurderet ud fra en potentiel konsekvens og sandsynlighed og omfatter risicienes tilgængelighed og fortrolighed. Vi har inspiceret, at sårbarheden af systemer og processer vurderes ud fra identificerede trusler. Vi har inspiceret, at serviceleverandøren har gennemført en risikovurdering inden for det seneste år. Vi har inspiceret, at serviceleverandøren har implementeret handlingsplaner for at reducere og minimerer de identificeret risici.	Ingen afvigelser konstateret

A.5 Organisatoriske foranstaltninger			
Kontrolmål	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
Politikker for informationssikkerhed At sikre løbende egnethed, tilstrækkelighed, effektivitet af ledelsens retning og støtte til informationssikkerhed i overensstemmelse med forretningsmæssige, juridiske, lovmæssige, regulatoriske og kontraktlige krav, i henhold til ISO/IEC 27002 A.5.1.	▶ Serviceleverandøren har udarbejdet og implementeret en informationssikkerhedspolitik. ▶ Serviceleverandørens informationssikkerhedspolitik bliver gennemgået og opdateret minimum en gang årligt.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og har observeret, at den er blevet godkendt inden for det seneste år.	Ingen afvigelser konstateret.
Roller og ansvar for informationssikkerhed At etablere en defineret, godkendt og forstået struktur for implementering, drift og styring af informationssikkerhed i organisationen, i henhold til ISO/IEC 27002 A.5.2.	▶ Serviceleverandøren sikrer, at samme person ikke har adgang til at tilgå, ændre og anvende systemer, informationer eller infrastruktur, uden at dette er godkendt eller vil blive opdaget. ▶ Serviceleverandøren har en klar opdeling af organisationen i forhold til informationssikkerhed og har udførlige ansvars- og rollebeskrivelser for de enkelte medarbejdere.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for rolle og ansvarsfordeling og har observeret, at ansvar og roller er tydeligt opdelt i organisationen. Vi har inspiceret serviceleverandørens udtræk over organisationens ansatte medarbejdere og har observeret, at der er en klar rollefordeling som er afspejlet i deres adgange og rettighedsniveau til organisationens respektive systemer.	Ingen afvigelser konstateret.
Funktionsadskillelse At reducere risikoen for svindel, fejl og omgåelse af informationssikkerhedsforanstaltninger, i henhold til ISO/IEC 27002 A.5.3.	▶ Serviceleverandørens funktioner og ansvarsområder er adskilt, i det omfang det er muligt taget virksomhedens størrelse i betragtning, for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af data.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for rolle og ansvarsfordeling og har observeret, at ansvar og roller er tydeligt opdelt i organisationen.	Ingen afvigelser konstateret.

		Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og øvrige emnespecifikke politikker og procedurer og har observeret, at der er funktionsadskillelse mellem medarbejder der har udarbejdet proceduren og direktøren, som har godkendt en denne. Vi har inspiceret serviceleverandørens udtræk over organisationens ansatte medarbejdere og har observeret, at der er en klar funktionsadskillelse, som er afspejlet i deres adgange og rettighedsniveau til organisationens respektive systemer.	
Ledelsens ansvar At sikre, at ledelsen har forstået deres informationssikkerhedsmæssige rolle og iværksætter handlinger for at sikre, at alle medarbejdere er bevidste om og opfylder deres informationssikkerhedsansvar, i henhold til ISO/IEC 27002 A.5.4.	▶ Ledelsen sikrer, at alle medarbejdere og relevante leverandører er orienteret og opretholder serviceleverandørens krav til informationssikkerhed.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og har observeret, at der er udformet formelle krav for overholdelse af informationssikkerhed for medarbejderne. Vi har på forespørgsel fået oplyst, at serviceleverandøren årligt sikre, at alle medarbejdere har bekræftet, at de har læst, forstået og følger organisationens informationssikkerhedspolitik. Vi har inspiceret, at medarbejderne har læst, forstået og følger informationssikkerhedspolitikken.	Ingen afvigelser konstateret.

Fortegnelse over information og understøttende aktiver At klarlægge organisationens information og understøttende aktiver for at bevare informationssikkerhed og tildele passende ejerskab, i henhold til ISO/IEC 27002 A.5.9.	▶ Serviceleverandøren har en fortegnelse over aktiver, der anvendes til udførelse af serviceleverandørens aktiviteter (dette inkluderer ansattes udstyr). ▶ Anvendte aktiver er tildelt en ejer.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for styring og beskyttelses af aktiver og har observeret, at aktiver skal registreres og tildeles en ejer. Vi har inspiceret serviceleverandørens register over aktiver og har observeret, at infrastruktur såvel som medarbejderudstyr er registeret. Vi har inspiceret, at aktiver, er tildelt en ejer.	Ingen afvigelser konstateret.
Administration af adgange At sikre autoriseret adgang og forhindre uautoriseret adgang til information og understøttende aktiver, i henhold til ISO/IEC 27002 A.5.15.	▶ Serviceleverandøren har udarbejdet en procedure for adgangsstyring, som styrer registreringer og afmeldinger af brugeradgange. ▶ Serviceleverandøren har kun givet medarbejdere adgang til netværk og netværkstjenester, som de er autoriseret til at anvende.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring. Vi har inspiceret at tildeling af adgange og rettigheder for nye medarbejdere er sket i overensstemmelse med serviceleverandørens procedure. Vi har på forespørgsel fået oplyst, at der i perioden op til erklæringsdatoen ikke har været fratrædelser, hvorfor implementeringen af kontrolaktiviteten ikke kunne testes.	Vi har konstateret, at der ikke har været afmelding af brugere i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering. Ingen afvigelser konstateret.

Styring af identifikation At give mulighed for entydig identifikation af personer og systemer, der får adgang til organisationens information og understøttende aktiver, og at muliggøre passende tildeling af adgangsrettigheder, i henhold til ISO/IEC 27002 A.5.16.	▶ Serviceleverandøren har opstillet en procedure for registrering og afmelding af bruger i forbindelse med tildeling af adgangsrettigheder.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring og har observeret, at der er en formel arbejdsgang for oprettelse, ændringer, nedlæggelser. Vi har for en stikprøve inspiceret at tildeling af adgange og rettigheder for nye medarbejdere er sket i overensstemmelse med serviceleverandørens procedure. Vi har inspiceret serviceleverandørens oversigt over ansatte og observeret, at medarbejdere har fået tildelt adgange og rettighedsniveau som er passende til deres arbejdsbehov. Vi har på forespørgsel fået oplyst, at der efter procedurens implementering ikke har været fratrædelser.	Vi har konstateret, at der ikke har været afmelding af brugere i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering. Ingen afvigelser konstateret.
Autentifikationsoplysninger At sikre korrekt entitetsautentifikation og forhindre fejl i autentifikationsprocesser, i henhold til ISO/IEC 27002 A.5.17.	▶ Serviceleverandøren har etableret regler for krav til adgangskoder, som skal følges af alle medarbejdere samt eksterne konsulenter. ▶ Serviceleverandøren har opstillet systemer til administration af adgangskoder, og disse er aktive. ▶ Serviceleverandøren styrer tildeling af hemmelig autentifikationsinformation ved hjælp af en formel administrationsproces.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og har observeret, at der er opsat regler for adgangskoder som følger best practise standarder. Vi har inspiceret serviceleverandørens konfiguration for adgangskoder og har observeret, at	Vi har konstateret, at der ikke har været anvendt eksterne konsulenter i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering. Ingen afvigelser konstateret.

		opsætningen følger serviceleverandørens krav i deres informationssikkerhedspolitik. Vi har inspiceret serviceleverandørens system for til administration af adgangskoder og har observeret, at serviceleverandørens kunder er omfattet af denne løsning og følger serviceleverandørens regler og opsætning af adgangskoder. Vi har inspiceret, at serviceleverandøren styrer tildeling af hemmelig autentifikationsinformation ved hjælp af en formaliseret administrationsproces.	
Adgangsrettigheder At sikre, at adgang til information og understøttende aktiver er defineret og autoriseret overensstemmelse med de forretningsmæssige krav, i henhold til ISO/IEC 27002 A.5.18.	▶ Serviceleverandøren har opstillet en procedure for adgangsstyring af tildeling og tilbagekaldelse af adgangsrettigheder. ▶ Serviceleverandøren foretager periodisk gennemgang af brugers adgangsrettigheder. ▶ Serviceleverandøren inddrager og tilpasser adgangsrettigheder, når medarbejdere fratræder eller aftaler ophører.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring og har observeret, at der er en formel arbejdsgang for oprettelse, ændringer, nedlæggelser og periodisk gennemgang adgangsrettigheder. Vi har inspiceret at tildeling af adgange og rettigheder for nye medarbejdere er sket i overensstemmelse med serviceleverandørens procedure. Vi observeret, at der er udført en periodisk gennemgang af adgangsrettigheder. Vi har på forespørgsel fået oplyst, at der ikke har været tilbagekaldelse af adgangsrettigheder i	Vi har konstateret, at der ikke har været tilbagekaldelse af adgangsrettigheder i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering. Ingen afvigelser konstateret.

		perioden op til erklæringsdatoen.	
Informationssikkerhedspolitik i leverandørforhold At opretholde et aftalt informationssikkerhedsniveau i leverandørforhold, i henhold til ISO/IEC 27002 A.5.19.	▶ Serviceleverandøren har fastsat informationssikkerhedskrav til anvendte underleverandører. ▶ Serviceleverandøren har begrænset underleverandørers adgang til serviceleverandørens systemer i forhold til underleverandørens arbejdsbetingede behov.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for leverandørstyring og har observeret, at der udarbejdet formelle krav til leverandørens sikkerhed, som kræves i forbindelse med et samarbejde mellem leverandør og serviceleverandøren. Vi har inspiceret indgået aftaler med underleverandører og har observeret, at der er indgået aftale med formelle krav til sikkerhed. Vi har på forespørgsel fået oplyst, at underleverandøren ikke har adgang til serviceleverandørens systemer.	Ingen afvigelser konstateret.
Håndtering af informationssikkerhed i leverandørforhold At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne, i henhold til ISO/IEC 27002 A.5.20.	▶ Informationssikkerhedskrav er aftalt med relevante underleverandører.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for leverandørstyring og har observeret, at der udarbejdet formelle krav til leverandørens sikkerhed som kræves i forbindelse med et samarbejde mellem leverandør og serviceleverandøren.	Ingen afvigelser konstateret.

		Vi har inspiceret indgået aftaler med underleverandører og har observeret, at der er indgået aftale med formelle krav til sikkerhed.	
Overvågning, vurdering og ændringsstyring i leverandørydelser At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne, i henhold til ISO/IEC 27002 A.5.22.	▶ Serviceleverandøren udfører tilsyn, herunder indhenter og gennemgår underserviceleverandørens revisorerklæringer, certificeringer og lignende. ▶ Serviceleverandøren udfører tilsyn af underserviceleverandører baseret på en risikovurdering. ▶ Serviceleverandøren udfører tilsyn af underserviceleverandører minimum en gang om året, baseret på en risikovurdering. ▶ Serviceleverandøren tager stilling til eventuelle ændringer af leverandørydelser.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for leverandørstyring og har observeret, at der for relevante leverandører skal udarbejdes en tilsynsvurdering mindst én gang om året. Vi har inspiceret serviceleverandørens register over leverandører og har observeret, alle leverandører er risikovurderet, som afspejler hvordan serviceleverandøren udfører tilsyn med leverandørerne. Vi har inspiceret, at der er gennemført tilsyn med underleverandører. Vi har på forespørgsel fået oplyst, at der efter procedurens implementering ikke har været tilfælde med ændringer, nedlæggelser eller tilføjelser af leverandørydelser, hvorfor kontrolaktivitetens implementering ikke kunne testes.	Vi har konstateret, at der ikke har været ændringer, nedlæggelser eller tilføjelser af leverandørydelser i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering. Ingen afvigelser konstateret.
Planlægning og forberedelse af incidenthåndtering ved sikkerhedsincidents At sikre hurtig, effektiv, konsekvent og velordnet håndtering af informationssikkerhedsincidents, herunder kommunikation om informationssikkerhedshændelser, i henhold til ISO/IEC 27002 A.5.24.	▶ Der er fastlagt ledelsesansvar og roller i forbindelse med brud på informationssikkerheden.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedurer for håndtering af IT-sikkerhedshændelser.	Vi har konstateret, at der ikke har været hændelser i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering.

	▶ Serviceleverandøren har implementeret en procedure for håndtering af brud på informationssikkerheden.	Vi har inspiceret serviceleverandørens hændelseslog og har observeret, at der ikke har været hændelser.	Ingen afvigelser konstateret.
Dokumenterede driftsprocedurer At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter, i henhold til ISO/IEC 27002 A.5.37.	▶ Driftsprocedurer er udarbejdet og gjort tilgængelige for relevante ansatte.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens elektroniske dokumentationsmiljø og har observeret, af serviceleverandørens driftsprocedure er offentligt tilgængelig for serviceleverandørens medarbejdere.	Ingen afvigelser konstateret.

A.6 Personrelaterede foranstaltninger			
Kontrolmål	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
Screening At sikre, at alle medarbejdere er egnet til de roller, som de er i betragtning til, og forbliver egnede under deres ansættelse, i henhold til ISO/IEC 27002 A.6.1.	▶ Serviceleverandøren udfører screening af potentielle medarbejdere før ansættelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for on/offboarding og har observeret, at der i forbindelse med ansættelser skal udføres en passende screening af den nye medarbejder. Vi inspiceret, at serviceleverandøren har udført en passende screening i forbindelse med ansættelse af en ny medarbejder.	Ingen afvigelser konstateret.
Awareness, uddannelse og træning vedrørende informationssikkerhed At sikre, at medarbejdere og relevante interessenter er bevidste om og lever op til deres informationssikkerhedsansvar, i henhold til ISO/IEC 27002 A.6.3.	▶ Serviceleverandøren afholder awareness-træning ved ansættelse af nye medarbejdere i henhold til informationssikkerhed. ▶ Der afholdes introduktionskursus for nye medarbejdere om informationssikkerhed. ▶ Serviceleverandøren foretager løbende awareness-træning og quizzer af medarbejdere i henhold til informationssikkerhed samt håndteringen heraf.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for onboarding og har observeret, at der i forbindelse med ansættelser skal ske en sikkerhedsrelevant træning med fokus på informationssikkerhedspolitikker og emne specifikke procedurer. Vi inspiceret, at der i forbindelse med onboarding af ny medarbejder er blevet udført sikkerhedsrelevant træning i overensstemmelse med serviceleverandørens onboarding procedurer.	Ingen afvigelser konstateret.

		Vi har inspiceret serviceleverandørens læringsplatform og har observeret, at alle medarbejderen hos serviceleverandøren løbende gennemfører sikkerhedsrelevante træningsmoduler.	
Distancearbejde (fjernarbejde) At sikre informationssikkerheden, når medarbejdere arbejder på afstand, i henhold til ISO/IEC 27002 A.6.7.	▶ Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret antivirus. ▶ Fjernadgang til serviceleverandørens systemer og data sker via en krypteret forbindelse. ▶ Fjernadgang skal foregå via to-faktor autentifikation.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedurer for IT-sikkerhed og har observeret, at alle end-point enheder skal beskyttes med tekniske foranstaltninger. Vi har inspiceret et udtræk over serviceleverandørens status over implementeret antivirus beskyttelse og har observeret, at alle serviceleverandørens end-points er inkluderet. Vi har inspiceret serviceleverandørens krypteringsmetode til fjernadgang og har observeret, at der benyttet en tilstrækkelig stærk krypteringsmetode til brug af fjernadgang. Vi har inspiceret serviceleverandørens brug af MFA i forbindelse med fjernadgang og har observeret, at der er implementeret MFA ved forbindelse med fjernadgang.	Ingen afvigelser konstateret.
Indrapportering af informationssikkerhedshændelser At understøtte rettidig, konsistent og effektiv indrapportering af informationssikkerhedshændelser, som kan identificeres af medarbejdere, i henhold til ISO/IEC 27002 A.6.8.	▶ Serviceleverandøren rapporterer om informationssikkerhedshændelser til relevante parter.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for håndtering af IT-sikkerhedshændelser	Vi har konstateret, at der ikke har været hændelser i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering.

	▶ Serviceleverandøren rapporterer om informationssikkerhedssvagheder til relevante parter.	og har observeret, at der er formelle krav til rapportering af hændelser og svagheder til relevante interessenter. Vi har inspiceret serviceleverandørens hændelseslog og har observeret, at der ikke har været hændelser.	Ingen afvigelser konstateret.

A.7 Fysiske foranstaltninger			
Kontrolmål	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
Fysisk områdesikring At forhindre uautoriseret fysisk adgang til, beskadigelse og forstyrrelse af organisationens information og understøttende aktiver, i henhold til ISO/IEC 27002 A.7.1	▶ Der er etableret fysisk områdesikring til at beskytte områder, der indeholder følsomme og kritiske informationer.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for IT-sikkerhed og har observeret, at der er etableret fysiske sikkerhedsforanstaltninger for serviceleverandørens fysiske bygninger. Vi har observeret, at der ved serviceleverandørens bygning er implementeret et alarmsystem. Vi har inspiceret serviceleverandørens underleverandør InterXion's SOC 2 erklæring og har observeret, at den er gældende fra den 01.01.2023 til den 31.12.2023. Vi har inspiceret serviceleverandørens underleverandør, Fuzion's, ISAE 3402 erklæring og har observeret, at den er gældende fra den 01.07.2023 til den 28.02.2025. Vi har inspiceret begge underleverandørs uafhængige revisor rapporter og har observeret, at der i begge tilfælde ikke har været afvigelser, som har påvirket serviceleverandørens fysiske sikkerhed.	Ingen afvigelser konstateret.

Fysisk adgangskontrol At sikre, at der kun sker autoriseret fysisk adgang til organisationens information og understøttende aktiver, i henhold til ISO/IEC 27002 A.7.2	▶ Der er etableret fysiske adgangskontroller, som forebygger sandsynligheden for uautoriseret adgang til serviceleverandørens kontorer og faciliteter, herunder sikring, at kun autoriserede personer har adgang. ▶ Der foretages løbende og som minimum en gang om året gennemgang af den fysiske adgang til serviceleverandørens kontorer og faciliteter.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for IT-sikkerhed og har observeret, at fysiske sikkerhedsforanstaltninger for serviceleverandørens fysiske bygninger. Vi har observeret, at der ved serviceleverandørens bygning er implementeret et alarmsystem. Vi har inspiceret, at der er foretaget periodisk gennemgang af adgangene.	Ingen afvigelser konstateret.
Beskyttelse mod fysiske og miljømæssige trusler At forebygge eller reducere konsekvenserne af hændelser, der opstår på grund af fysiske og miljømæssige trusler, i henhold til ISO/IEC 27002 A.7.5.	▶ Serviceleverandøren har etableret kontroller til beskyttelse mod eksterne og miljømæssige trusler, herunder efterlevelse af specificerede krav til serverrum.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for IT-sikkerhed og har observeret, at fysiske sikkerhedsforanstaltninger er omfattet. Vi har på forespørgsel fået oplyst, at serviceleverandøren har outsourcet de områder i deres infrastruktur som skal beskyttes mod miljømæssige trusler, til deres underleverandører. Vi har inspiceret serviceleverandørens underleverandør InterXion's SOC 2 erklæring og har observeret, at den er gældende fra den 01.01.2023 til den 31.12.2023. Vi har inspiceret serviceleverandørens underleverandør, Fuzion's, ISAE 3402 erklæring og har	Ingen afvigelser konstateret.

		observeret, at den er gældende fra den 01.07.2023 til den 28.02.2025. Vi har inspiceret begge underleverandørs uafhængige revisor rapporter og har observeret, at der i begge tilfælde ikke har været afvigelser, som har påvirket serviceleverandørens fysiske sikkerhed.	
Placering og beskyttelse af udstyr At reducere risici fra fysiske og miljømæssige trusler og fra uautoriseret adgang og beskadigelse, i henhold til ISO/IEC 27002 A.7.8.	▶ Serviceleverandøren har sikret, at udstyr er placeret i sikre lokaler for at beskytte mod uautoriserede adgange og miljømæssige trusler.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for IT-sikkerhed og har observeret, at fysiske sikkerhedsforanstaltninger er omfattet. Vi har observeret, at der ved serviceleverandørens bygning er implementeret et alarmsystem. Vi har inspiceret serviceleverandørens fortegnelse over medarbejdere med autoriseret adgang og har observeret, at det kun er medarbejdere med et arbejdsbetinget behov som fremkommer af listen. Vi har på forespørgsel fået oplyst, at serviceleverandøren har outsourcet de områder i deres infrastruktur som skal beskyttes mod miljømæssige trusler, til deres underleverandører. Vi har inspiceret serviceleverandørens underleverandør InterXion's SOC 2 erklæring og har observeret, at den er gældende fra den 01.01.2023 til den 31.12.2023.	Ingen afvigelser konstateret.

		Vi har inspiceret serviceleverandørens underleverandør, Fuzion's, ISAE 3402 erklæring og har observeret, at den er gældende fra den 01.07.2023 til den 28.02.2025. Vi har inspiceret begge underleverandørs uafhængige revisor rapporter og har observeret, at der i begge tilfælde ikke har været afvigelser, som har påvirket serviceleverandørens fysiske sikkerhed.	
Forsyningssikkerhed At undgå tab, beskadigelse eller kompromittering af information og understøttende aktiver eller driftsforstyrrelser i organisationen som følge af fejl og afbrydelse af understøttende forsyninger, i henhold til ISO/IEC 27002 A.7.11.	▶ Udstyr er beskyttet mod strømsvigt og andre forstyrrelser.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for IT-sikkerhed og har observeret, at serviceleverandøren stiller krav til serviceleverandørens underleverandørens fysiske sikkerhed som kan påvirke serviceleverandøren. Vi har på forespørgsel fået oplyst, at serviceleverandøren har outsourcet de områder i deres infrastruktur som skal beskyttes mod forsynings trusler, til deres underleverandører. Vi har inspiceret serviceleverandørens underleverandør InterXion's SOC 2 erklæring og har observeret, at den er gældende fra den 01.01.2023 til den 31.12.2023. Vi har inspiceret serviceleverandørens underleverandør, Fuzion's, ISAE 3402 erklæring og har observeret, at den er gældende fra den 01.07.2023 til den 28.02.2025.	Ingen afvigelser konstateret.

		Vi har inspiceret begge underleverandørs uafhængige revisor rapporter og har observeret, at der i begge tilfælde ikke har været afvigelser, som har påvirket serviceleverandørens forsyningssikkerhed.	
Vedligeholdelse af udstyr At undgå tab, beskadigelse, tyveri eller kompromittering af information og understøttende aktiver samt driftsforstyrrelser i organisationen grundet manglende vedligeholdelse, i henhold til ISO/IEC 27002 A.7.13.	▶ Vedligeholdelse af udstyr følger en vedligeholdelsesplan og udføres kun af autoriseret personale.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure og observeret at udskiftning af udstyr er omfattet af formelle krav og eventuelle ændringer skal ske gennem en godkendelsesproces, før den bliver implementeret. Vi har inspiceret serviceleverandørens overvågningssystem og har observeret, at systemet alarmerer serviceleverandøren når udstyr skal optimeres eller udskiftes. Vi har inspiceret serviceleverandørens fortegnelse over medarbejdere og har observeret, at der forekommer en liste over medarbejdere som er autoriseret til at kunne udskifte udstyr. Vi har på forespørgsel fået oplyst, at der ikke har været hændelser i periodens op til erklæringsdatoen.	Vi har konstateret, at der ikke har været udskiftning eller vedligeholdelse af fysisk udstyr i perioden op til erklæringsdatoen, hvorfor vi ikke har kunne teste kontrollens implementering. Ingen afvigelser konstateret.

A.8 Teknologiske foranstaltninger			
Kontrolmål	**Kontrolaktivitet**	**Test udført af BDO**	**Resultat af test**
Privilegerede adgangsrettigheder At sikre, at kun autoriserede brugere, softwarekomponenter og -tjenester har privilegerede adgangsrettigheder, i henhold til ISO/IEC 27002 A.8.2.	▶ Privilegerede (administrative) adgangsrettigheder til software, systemer og enheder tildeles ud fra arbejdsbetinget behov.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedurer for adgangsstyring og har observeret, at adgangsrettigheder tildeles ud fra et arbejdsbetinget behov. Vi har inspiceret serviceleverandørens fortegnelse over medarbejdere, aktiver og systemer og har observeret, at der for hver medarbejder er angivet et rettighedsniveau til serviceleverandørens systemer og aktiver. Vi har inspiceret, serviceleverandørens fortegnelse observeret, at brugere med privilegerede rettigheder alle har et arbejdsbetinget behov.	Ingen afvigelser konstateret.
Begrænset adgang til informationer At sikre udelukkende autoriseret adgang og forhindre uautoriseret adgang til information og understøttende aktiver, i henhold til ISO/IEC 27002 A.8.3.	▶ Serviceleverandøren har begrænset medarbejderes adgang til kundernes informationer, aktiver og systemer ud fra et arbejdsbetinget behov.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedurer for adgangsstyring og har observeret, at adgangsrettigheder tildeles ud fra et arbejdsbetinget behov. Vi har inspiceret serviceleverandørens fortegnelse over medarbejdere, aktiver og systemer og har observeret, at der for hver medarbejder	Ingen afvigelser konstateret.

		er angivet et rettighedsniveau til serviceleverandørens systemer og aktiver. Vi har inspiceret, at serviceleverandøren har begrænset medarbejderes adgang til kundernes informationer, aktiver og systemer ud fra et arbejdsbetinget behov.	
Sikker autentifikation At sikre, at en bruger eller en entitet autentificeres på sikker vis, når der gives adgang til systemer, applikationer og tjenester, i henhold til ISO/IEC 27002 A.8.5.	▶ Serviceleverandøren har etableret logisk adgangskontrol til systemer med informationer, herunder to-faktor autentifikation.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for adgangsstyring herunder krav til adgangskoder. Vi har inspiceret serviceleverandørens tekniske opsætning af logisk adgangskontrol og har observeret, at den følger serviceleverandørens procedure. Vi har inspiceret, at der ved login til systemer og informationer er påkrævet godkendelse med to-faktor-autentifikation.	Ingen afvigelser konstateret.
Beskyttelse mod malware At sikre, at information og understøttende aktiver beskyttes mod malware, i henhold til ISO/IEC 27002 A.8.7.	▶ Der er implementeret kontroller til detektering, forhindring og gendannelse kombineret med passende brugerbevidsthed for at beskytte mod malware.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for IT-sikkerhed og har observeret, at alle virksomhedens end-points skal være beskyttet med antivirus.	Ingen afvigelser konstateret.

		Vi har inspiceret serviceleverandørens end-points og har observeret, at der er implementeret en opdateret antivirus beskyttelse. Vi har inspiceret, at der er installeret antivirus beskyttelse på kundernes infrastruktur. Vi har inspiceret serviceleverandørens lærings platform og har observeret, at der forekommer et modul som omfatter antivirus beskyttelse. Vi har inspiceret et udtræk over at serviceleverandørens medarbejdere har gennemført bevidsthedstræning indenfor malwarebeskyttelse.	
Styring af tekniske sårbarheder At forhindre, at tekniske sårbarheder udnyttes, i henhold til ISO/IEC 27002 A.8.8.	▶ Serviceleverandøren indhenter informationer om tekniske sårbarheder. ▶ Serviceleverandøren har taget stilling til identificerede sårbarheder.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens seneste sårbarhedsskanning og har observeret, at den er udført inden for det seneste år. Vi har inspiceret serviceleverandørens har taget stilling til identificerede sårbarheder.	Ingen afvigelser konstateret.
Konfigurationsstyring At sikre, at hardware, software, tjenester og netværk fungerer korrekt med de krævede sikkerhedsindstillinger og at der ikke laves om på konfigurering ved uautoriserede eller ukorrekte ændringer, i henhold til ISO/IEC 27002 A.8.9.	▶ Serviceleverandøren sørger for hardware, software, tjenester og netværk fungerer korrekt i forhold til sikkerhedsindstillinger, som de har prædefineret samt sørger for at disse konfigurationer ikke kan ændres.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for system drift og har observeret, at der forekommer formelle krav og retningslinjer for sikker konfiguration, af serviceleverandørens systemer og aktiver.	Ingen afvigelser konstateret.

		Vi inspiceret, at der i konfigurationsdokumentation), hvor man sikre sig en sikker konfiguration af systemet.	
Backup af information At muliggøre retablering efter tab af data eller systemer, i henhold til ISO/IEC 27002 A.8.13.	▶ Der foretages dagligt backup af systemer og data. ▶ Der udføres restore-tests mindst én gange årligt for kunder med aftale herom.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret at serviceleverandørens kontrollerende miljø og firewalls bliver sikkerhedskopieret på daglig basis. Vi har inspiceret at der for kunder foretages daglig backup. Vi har inspiceret serviceleverandørens backup konfiguration og har observeret, at der dagligt sendes besked til relevant personale i tilfælde af fejlede backup, som reagerer og håndtere notifikationer når det er nødvendigt. Vi har på forespørgsel fået oplyst, at der foretages restore test for kunder, som har efterspurgt dette. Vi har for inspiceret at serviceleverandøren efter instruks fra kunden har gennemført restore test på et kundemiljø.	Ingen afvigelser konstateret.
Logning At optegne hændelser, generere bevismateriale, sikre loginformationens integritet, forhindre uautoriseret adgang, identificere informationssikkerhedshændelser, der kan føre til et	▶ Alle succesfulde og mislykkede adgangsforsøg til systemleverandørens systemer og data logges. ▶ Alle brugerændringer i system og databaser logges.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens udtræk over logfiler for logisk adgangskontrol og har	Ingen afvigelser konstateret.

informationssikkerhedsincident og understøtte undersøgelser, i henhold til ISO/IEC 27002 A.8.15.	▶ Serviceleverandøren har begrænset, hvem der kan få adgang til logdata. ▶ Serviceleverandøren logger administrator- og operatøraktiviteter. ▶ Loggen slettes efter den fastsatte retentionsperiode.	observeret, at både succesfulde og fejlede log-inforsøg logges og gemmes. Vi har inspiceret serviceleverandørens audit log og har observeret, at brugerhandlinger logges og gemmes. Vi har inspiceret serviceleverandørens fortegnelse over medarbejdere, aktiver og systemer og har observeret, at adgang til logfiler er begrænset til medarbejdere med et arbejdsbetinget behov. Vi har inspiceret serviceleverandørens logfiler for logisk adgangskontrol og brugerhandlinger og har observeret, at der ikke forekommer logfiler som overskrider serviceleverandørens slettefrist.	
Brug af privilegerede understøttende programmer At sikre, at brugen af understøttende programmer ikke skader system- og applikationsforanstaltninger til informationssikkerhed, i henhold til ISO/IEC 27002 A.8.18.	▶ Kun autoriserede medarbejdere kan anvende programmer, der kan omgå system- og applikationskontroller.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og har observeret, at der er klare krav og regler for acceptabelt brug af virksomhedsudstyr og installering af software. Vi har inspiceret serviceleverandørens systembeskrivelse og har observeret, at brugere ikke har lokale administratorrettigheder på deres arbejdsstationer. Vi har inspiceret medarbejdernes arbejdsstationer og har observeret, at der	Ingen afvigelser konstateret.

		ikke er lokaleadministrator rettigheder på enhederne, og at det er påkrævet at anmode om softwareinstallering som skal begrundes.	
Softwareinstallationer At sikre integriteten af test- og produktionssystemer og forhindre udnyttelse af tekniske sårbarheder, i henhold til ISO/IEC 27002 A.8.19.	▶ Serviceleverandøren har implementeret procedurer for softwareinstallation. ▶ Serviceleverandøren har opstillet regler for softwareinstallationer.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og har observeret, at der er klare krav og regler for acceptabelt brug af virksomhedsudstyr og installering af software. Vi har inspiceret medarbejdernes arbejdsstationer og har observeret, at der ikke er lokaleadministrator rettigheder på enhederne, og at det er påkrævet at anmode om softwareinstallering som skal begrundes.	Ingen afvigelser konstateret.
Netværkssikkerhed At beskytte informationer i netværk og understøttende informationsbehandlingsfaciliteter mod kompromittering via netværket, i henhold til ISO/IEC 27002 A.8.20.	▶ Netværkstopologien er struktureret således at servere som driver applikationer ikke kan tilgås direkte fra internettet. ▶ Serviceleverandøren anvender kendte netværksteknologier og mekanismer for at beskytte serviceleverandørens interne netværk.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens netværkstopologi og har observeret, at netværket er segmenteret. Vi har inspiceret serviceleverandørens firewall opsætning og har observeret, at den er opsat med passende regler. Vi har inspiceret et udtræk over serviceleverandørens liste over kunder og kundernes opsætningsregler på deres firewall.	Ingen afvigelser konstateret.

		Vi har inspiceret, at firewallopsætningen for serviceleverandørens kunder er i overensstemmelse med kundens opsætningsregler.	
Sikring af netværkstjenester At sørge for sikkerhed i brugen af netværkstjenester, i henhold til ISO/IEC 27002 A.8.21.	▶ Serviceleverandøren har implementeret/stillet krav til passende sikkerhedsforanstaltninger til beskyttelse af dens netværkstjenester.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedure for firewalls, switches og vlans og har observeret, at der er opsat krav og retningslinjer for installation, konfigurering, drift, vedligeholdelse, kapacitetsstyring og monitorering af netværkskomponenter og deres tjenester. Vi har observeret, at serviceleverandørens netværk er sikret i overensstemmelse med deres procedure.	Ingen afvigelser konstateret.
Segmentering af netværk At inddele netværket med sikkerhedsafgrænsninger og styre trafikken mellem dem ud fra forretningsmæssige behov, i henhold til ISO/IEC 27002 A.8.22.	▶ Serviceleverandørens netværk er segmenteret, så interne servere ikke kommunikerer direkte med internettet.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens netværkstopologi og har observeret, at netværket er segmenteret. Vi har inspiceret serviceleverandørens firewall opsætning og har observeret, at den er opsat med passende regler som forhindrer trafik til og fra internettet i at kommunikere direkte med serviceleverandørens infrastruktur.	Ingen afvigelser konstateret.

Ændringsstyring At bevare informationssikkerheden ved udførelse af ændringer, i henhold til ISO/IEC 27002 A.8.32.	▶ Serviceleverandøren har oprettet procedurer for systemændringer. ▶ Serviceleverandøren foretager passende test af nye systemændringer. ▶ Serviceleverandøren har opstillet regler for begrænsninger af softwareinstallationer.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens procedurer for ændringsstyring og har observeret, at der er formelle krav og retningslinjer for systemændringer som omfatter test og godkendelse af ændringer. Vi har inspiceret, at der er foretaget ledelsesgodkendelse samt test før en ændring implementeres. Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og har observeret, at der er formelle krav og retningslinjer for installering af software. Vi har inspiceret, at der er påkrævet en godkendelse af installations anmodning før der kan installeres software for en arbejdsstation.	Ingen afvigelser konstateret.

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

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."

Jackie Nyberg Amelung
CEO
Serienummer: f221ba78-ae56-4e40-ae35-0b6f34082295
IP: 104.28.xxx.xxx
2025-03-19 16:45:54 UTC

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d
IP: 188.177.xxx.xxx
2025-03-19 17:27:24 UTC

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 62.66.xxx.xxx
2025-03-19 18:03:28 UTC