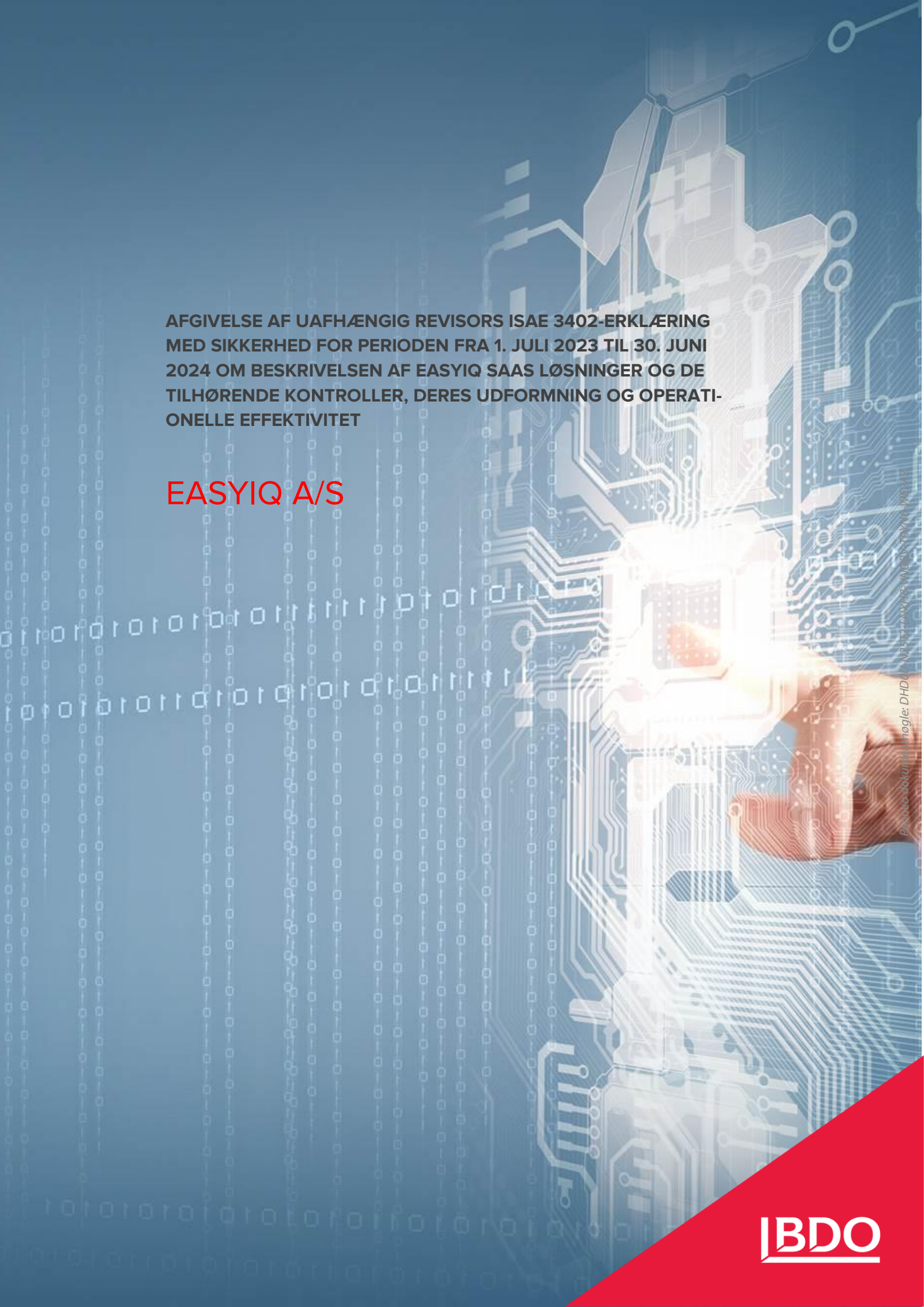
# AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JULI 2023 TIL 30. JUNI 2024 OM BESKRIVELSEN AF EASYIQ SAAS LØSNINGER OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

## EASYIQ A/S



Penneo dokumentnøgle: DHDCL-N2SZT-LWXH8-WNCDX-T0YNL-WMPAE

# INDHOLD



Penneo dokumentnøgle: DHDOU-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

# 1. UAFHÆNGIG REVISORS ERKLÆRING

## UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JULI 2023 TIL 30. JUNI 2024 OM BESKRIVELSEN AF EASYIQ SAAS LØSNINGER OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Til: Ledelsen i EasyIQ A/S
EasyIQ A/S' kunder og deres revisorer

### Omfang

Vi har fået som opgave at afgive erklæring om den af EasyIQ A/S (serviceleverandøren) for hele perioden fra 1. juli 2023 til 30. juni 2024 udarbejdede beskrivelse i sektion 3 af EasyIQ SaaS løsninger og de tilhørende kontroller, og om udformningen og den operationelle effektivitet af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

### 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, implementere og effektivt udføre 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 og den operationelle effektivitet 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 kontroller hos en serviceorganisation. 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 og fungerer effektivt.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, udformningen og den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse samt for kontrollernes udformning og operationelle effektivitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risicierne for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af den operationelle effektivitet 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 serviceleverandøren har specificeret og beskrevet i sektion 2.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

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 EasyIQ SaaS løsninger, 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. Herudover er fremskrivningen af enhver vurdering af den operationelle effektivitet af kontroller 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 serviceleverandørens udtalelse i sektion 2. Det er vores opfattelse:

a. at beskrivelsen af EasyIQ SaaS løsninger og de tilhørende kontroller, således som de var udformet og implementeret i hele perioden fra 1. juli 2023 til 30. juni 2024, 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 i hele perioden fra 1. juli 2023 til 30. juni 2024, og

c. at de testede kontroller, som var de, 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 perioden fra 1. juli 2023 til 30. juni 2024.

**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 EasyIQ SaaS løsninger, 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 1. juli 2024

**BDO Statsautoriseret revisionsaktieselskab**

Nicolai T. Visti
Partner, Statsautoriseret revisor

Brian Bomholdt
Partner, CISA, CISM, CISSP

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## 2. EASYIQ A/S' UDTALELSE

EasyIQ A/S leverer egenudviklede it-systemer som EasyIQ SaaS løsninger. Leverancen omfatter drift, service og support, konsulentydelser samt uddannelse og kurser. Hertil løbende tilpasninger af funktionalitet, således at systemerne lever op til gældende lovgivning og reguleringer.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt EasyIQ SaaS løsninger, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, når de opnår en forståelse af kunders informationssystemer, som er relevante for regnskabsaflæggelsen.

EasyIQ A/S anvender serviceunderleverandører. Disse serviceunderleverandørers relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

EasyIQ A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af EasyIQ SaaS løsninger og de tilhørende kontroller i hele perioden fra 1. juli 2023 til 30. juni 2024. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for EasyIQ SaaS løsninger, 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. Indeholder relevante oplysninger om ændringer i serviceleverandørens EasyIQ SaaS løsninger foretaget i perioden fra 1. juli 2023 til 30. juni 2024.
3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af EasyIQ SaaS løsninger 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 EasyIQ SaaS løsninger, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

EasyIQ A/S bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. juli 2023 til 30. juni 2024. 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.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

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.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden fra 1. juli 2023 til 30. juni 2024.

Skanderborg, den 1. juli 2024

**EasyIQ A/S**

**Frank Nygaard**
**Direktør**

Penneo dokumentnøgle: DHDOU-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

# 3. EASYIQ A/S' BESKRIVELSE AF EASYIQ SAAS LØSNINGER

**Indledning**

Formålet med nærværende beskrivelse er at levere information til EasyIQ A/S kunder og deres revisorer vedrørende kravene i ISAE 3402, som er den internationale revisorstandard for erklæringsopgaver om kontroller hos serviceleverandører. Desuden er formålet med beskrivelsen en afdækning af de tekniske og organisatoriske sikringsforanstaltninger, som er implementeret i forbindelse af driften af EasyIQ SaaS løsninger. Produktrammen for denne beskrivelse er følgende SaaS løsninger:

- EasyIQ SkolePortal – Læringsplatform med læringsforløb, opgaver, afleveringer, portfolio, skabeloner, Fælles Mål, Læringsmål samt Elevplan / Meddelelsesbog. Integreret med Microsoft 365 og Google Workspace.
- EasyIQ Dagtilbud – Læringsplatform med læringsforløb, opgaver, afleveringer, portfolio, skabeloner, Fælles Mål, Læringsmål samt Elevplan / Meddelelsesbog. Integreret med Office 365 og Google Workspace.
- EasyIQ Microsoft 365 – Fælles dokument og kommunikationsplatform. Office-pakke, fællesdrev, klassedrev, fildeling, mail, kalender, grupper, OneNote, OneNote Cass Notebook, Teams, Classroom, Stream (Video portal), Forms, web- og videokonferencer og meget mere med ægte Unilogin inkl. support.
- EasyIQ Google Workspace - Fælles dokument og kommunikationsplatform baseret på Google Apps med adgang til dokumenter, fællesdrev, Google Classroom samarbejdsmuligheder m.m. adgang via Unilogin inkl. support.
- EasyIQ UniRadius - Redundant radius validering i forhold til UNI-Login.
- EasyIQ Lectio2Unilogin - Synkronisering fra Lectio til Unilogin – vi står for dagligt at synkronisere Lectio til Unilogin for elever og ansatte.
- EasyIQ IdP2Lectio – Synkronisering af password fra EasyIQ IdP til Lectio – Så elever og ansatte kan servicere sig selv via EasyIQ IdP.
- EasyIQ Widgets – Widget til Aula – Skolernes nye forældrekommunikation.
- EasyIQ ASM - Med EasyIQ ASM (Apple School Manager) oprettes, vedligeholdes og nedlægges elever, ansatte og klasser i Apple School Manager helt automatisk på baggrund af data i jeres brugeradministration.
- EasyIQ Lightspeed - Med EasyIQ Lightspeed oprettes, vedligeholdes og nedlægges elever, ansatte og klasser i Lightspeed helt automatisk på baggrund af data i jeres brugeradministration.
- EasyIQ Kodeskift – website hvor brugerne kan skifte deres AD/EasyIQ password.
- EasyIQ IDP – Redundant Unilogin IDP-løsning tilkoblet Unilogin og MitID Erhverv (NemLog-in3).
- EasyIQ MitID Erhverv – Udstedelse og MitID Erhverv via Kodeskift inkl. opsætning af rettigheder i MitID Erhverv.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

- EasyIQ IDM – Brugerne, som omfatter ansatte, lærere, pædagogisk personale og elever, oprettes og vedligeholdes på skolens/Kommunes AD. Løsningen benyttes typisk i sammenhæng med EasyIQ Kodeskift og EasyIQ IDP.

- EasyIQ 2Faktor – 2 faktorløsning til Unilogin, Aula og EasyIQ SkolePortal.

- EasyIQ Hosted Administration - Organisationens it-infrastruktur i skyen. EasyIQ står for drift af infrastruktur og applikationer på kundesystemer.

I relation til beskyttelse af personoplysninger i ovenstående SaaS-løsninger er der udarbejdet en selvstændig ISAE3000 erklæring med beskrivelse af sikringsforanstaltninger hos EasyIQ i rollen som databehandler for de dataansvarlige kunder, der anvender SaaS-løsningerne.

**Beskrivelse af EasyIQ A/S**
EasyIQ A/S i sin nuværende form blevet etableret i 2014 og beskæftiger i dag ca. 10 medarbejdere. Fundamentet blev grundlagt med virksomheden Systemtech A/S tilbage i 2004. Grundlaget for succesen, dengang som nu, er agil udvikling af it-systemer i tæt samarbejde med brugerne, eksperter og udviklere med stor domæneviden. Vi har stor fokus på god og hurtig kunde support. Dette er den filosofi, der stadig udgør grundstenen i EasyIQ A/S.

EasyIQ A/S leverer egenudviklede it-systemer som software as a service. Leverancen omfatter drift, service og support, konsulentydelser samt uddannelse og kurser. Hertil løbende tilpasninger af funktionalitet således at systemerne lever op til gældende lovgivning og reguleringer. Alle vores systemer udvikles, drives og forvaltes af dygtige medarbejdere med base i Danmark.

EasyIQ A/S er kvalitetsbevidst og har fokus på at levere den aftalte løsning til tiden og til skole venlige priser. Vi arbejder efter fastlagte procedure, der sikrer ensartethed i vores arbejde og leverancer.

**Forretningsstrategi/ it-sikkerhedsstrategi**
Det er EasyIQ A/S strategi, at der i forretningen skal være indbygget den nødvendige sikkerhed, således at selskabet ikke påføres uacceptable risici. Som leverandør til privat og kommuner, arbejder EasyIQ A/S med informationssikkerhed på et forretningsstrategisk niveau. Målsætningen er at være en professionel produktleverandør, der har en skarp holdning til at passe på de data, kunderne betror os. Det er EasyIQ A/S holdning, at vi altid skal sikre overholdelse af gældende lovgivning og gøre, hvad der er teknisk og økonomisk muligt, for at sikre databehandlingens fortrolighed, integritet og tilgængelighed på et højt niveau.

Informationssikkerheden er i højsædet på alle niveauer af organisationen. Alle medarbejdere skal være vidende om vigtigheden af dette fokus og selv være medvirkende til løbende at forbedre arbejdet omkring sikkerhed.

Vores målsætning for informationssikkerheden er, at EasyIQ A/S gennemfører alle nødvendige aktiviteter for at sikre:

- **Tilgængelighed**: At opnå en høj tilgængelighed med høje oppetider og minimeret risiko for nedbrud.
- **Integritet**: At opnå en pålidelig og korrekt funktion og minimeret risiko for ukorrekt datagrundlag, f.eks. som følge af menneskelige og systemmæssige fejl eller udefrakommende hændelser.
- **Fortrolighed**: At sikre fortrolig databehandling, transmission og opbevaring af data, hvor kun autoriserede brugere har adgang.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

Det er EasyIQ A/S mål at opretholde et informationssikkerhedsniveau, der som minimum:

- Følger gældende lovgivning
- Følger god brancheskik
- Lever op til kundens ønsker, krav og forventninger til en professionel leverandør

EasyIQ A/S har omkring it-sikkerhedsstrategien valgt at tage udgangspunkt i ISO27001 og 2, og har således brugt ISO-metodikken til at implementere de relevante sikringsforanstaltninger inden for følgende områder:

- Informationssikkerhedspolitikker
- Organisering af informationssikkerhed
- Medarbejdersikkerhed
- Styring af aktiver
- Adgangsstyring
- Driftssikkerhed
- Kommunikationssikkerhed
- Anskaffelse, udvikling og vedligeholdelse
- af systemer
- Leverandørforhold
- Styring af informationssikkerhedsbrud
- Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Rammen for hvilke kontrolmål og underliggende kontrolpunkter (sikkerhedselementer), som EasyIQ A/S direktion har defineret relevant for arbejdet med et passende sikkerhedsmiljø, er nærmere beskrevet i sektion 4.

**EasyIQ A/S organisation og organisering af it-sikkerheden**
EasyIQ er inddelt i 3 afdelinger: ledelse, salg og IT som består af support og drift. Support modtager alle indkomne forespørgsler, og enten løser kundernes problemer, eller formidler opgaven videre til driftsafdelingen til bearbejdning.

Driftsafdelingen fungerer både som 2. line support for support, og håndterer herudover praktiske implementeringer af nye kunder, overvåger bestående driftsløsninger og andet forbundet med den daglige drift af vores IT-Miljø.

EasyIQ's kontrolmiljø reflekterer den stilling som direktionen har taget til betydningen af kontroller og den vægt, der lægges på kontroller i politikker, procedurer, metoder og organisatorisk struktur. Følgende er en beskrivelse af EasyIQ A/S kontrolmiljø og leverance af IT services:

**Ansvarsfordeling:**

- Bestyrelsen har uddelegeret informationssikkerhedsansvaret til direktøren.
- Direktør (CEO), ansvarlig for kontrakter, SLA, IT, Informationssikkerhed, databeskyttelse, risikostyring og daglig ledelse.
- Salgschef, Ansvarlig for salg
- Supportchef, Ansvarlig for Support og Drift, her under eksterne drift aftaler

Der afholdes Informationssikkerhedsmøde årligt, for at sikre fokus og opfølgning på informationssikkerheden og databeskyttelse.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

EasyIQ A/S arbejder med en struktureret metode for at sikre, at alle processer og politikker er beskrevet i vores kvalitetsstyringssystem og ISMS. Dette for at sikre uafhængighed af enkeltpersoner. Incidents eller afvigelser af it-sikkerhedsrelateret karakter behandles på månedlige kvalitetsstyringsmøder, på baggrund af faste procedurer for håndtering af afvigelser.

**Risikostyring I EasyIQ A/S**
Det er EasyIQ A/S politik, at de risici, der følger af selskabets aktiviteter, skal afdækkes eller begrænses til et sådant niveau, at selskabet vil kunne opretholde en normal drift. EasyIQ A/S gennemfører risikostyring og interne kontroller på flere områder og niveauer. Der gennemføres en årlig risiko- og trusselsvurdering.

EasyIQ A/S har indarbejdet faste procedurer for risikovurdering af forretningen. Vi sikrer dermed, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau. Risikovurdering foretages periodisk, samt når vi ændrer i eksisterende systemer eller implementerer nye systemer, som vi vurderes relevante i forbindelse med at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderingen ligger hos direktør og skal efterfølgende forankres og godkendes hos virksomhedens direktør.

**Håndtering af it-sikkerhed**
Direktøren hos EasyIQ A/S har det daglige ansvar for it-sikkerhed, og derved sikres det, at de overordnede krav og rammer for it-sikkerhed er overholdt. Gennem den centrale it-sikkerhedspolitik har direktør beskrevet EasyIQ A/S struktur for it-sikkerhed. It-sikkerhedspolitikken skal som minimum revideres én gang årligt.

EasyIQ A/S kvalitetsstyringssystem er defineret ud fra den overordnede målsætning om at levere stabil og sikker it-drift til kunderne. For at kunne gøre det, er det nødvendigt, at vi har indført politikker og procedurer, der sikrer, at vores leverancer er ensartede og gennemsigtige.

EasyIQ A/S it-sikkerhedspolitik er udarbejdet med reference til ovenstående og er gældende for alle medarbejdere og for alle leverancer. Ved fejl eller sikkerhedsbrist i vores driftsmiljø udbedres fejlen/sikkerhedshullet omgående. Direktionen sikrer medarbejdernes kendskab til politikker og gældende retningslinjer. Ved indgåelse af aftaler med eksterne parter sikres den fornødne information om it-sikkerheds-mæssige krav, indgåelse af tavshedserklæringer og lignende.

Alle servere og netværksenheder er dokumenteret i EasyIQ A/S dokumentationssystem. Her logges alle ændringer af vores system. Konfigurationsfiler til netværksenheder (firewall, routere, switche og lignende) ligger gemt i vores dokumentationssystem.

Sikkerhedspolitikken sætter de grundlæggende politikker for EasyIQ A/S infrastruktur og omhandler ikke forhold vedrørende specifikke produkter, ydelser eller brugere.
Sikkerhedspolitikken er udarbejdet, så EasyIQ A/S har ét fælles regelsæt. Dermed opnår vi et stabilt driftsmiljø og et højt sikkerhedsniveau. Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift.

På it-sikkerhedsområdet har EasyIQ A/S implementeret de nødvendige procedurer og kontroller, i forhold til de enkelte områder inden for ISO27002:2013, som er defineret i bilag 1, som viser sikkerhedsstrukturen og de kontrolmål, som er implementeret hos EasyIQ A/S.

Penneo dokumentnøgle: DHDOU-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

Informationssikkerhed ved brug af cloudtjenester
EasyIQ har fastlagt, hvilke informationsrisici, der er forbundet ved anvendelse af Cloud-tjenester.

EasyIQ har processer for anskaffelse, brug, styring og afslutning af brugen af cloudtjenester i overensstemmelse med organisationens informationssikkerhedskrav.

Funktionsadskillelse
EasyIQ 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.

**HR, medarbejdere og uddannelse**
Medarbejdernes domæneviden og kompetencer er en vigtig forudsætning for EasyIQ A/S forretning.
Det er vigtigt at vedligeholde og udbygge de kompetencer, vi råder over, så vi er i stand til at imødekomme udfordringerne i en omskiftelig branche. Vi arbejder med årlige samtaler for efter/videreuddannelse, og hvor der fastsættes mål for medarbejdernes ønsker til faglig udvikling.

HR-afdelingen arbejder med faste procedurer for bl.a. rekruttering og ansættelse og fratrædelser. Nye medarbejdere gennemgår et grundigt introduktionsforløb til virksomheden. Forløbet omfatter information i informationssikkerhed, der omhandler it-sikkerhedsregler, introduktion til informationssikkerhedsorganisationen, god it-adfærd samt dataklassifikation.

EasyIQ A/S medarbejdere har i begrænset omfang mulighed for at arbejde fra andre faciliteter end kontoret i Skanderborg. Virksomheden har udarbejdet en procedure, der beskriver regler og gode råd til fjernarbejdsplads. Vi har etableret tekniske foranstaltninger, der sikrer en krypteret opkobling til kontorfaciliteter. Adgang til backendsystemer og driftsmiljøer er teknisk begrænset.

Alle medarbejdere har en fortrolighedsklausul i deres ansættelseskontrakter. Som en del af vores fratrædelsesprocedure indgår en exit-samtale med nærmeste leder, hvor vi minder om, at fortrolighedsklausulen fortsat er gældende efter endt ansættelse.

For at sikre en kontinuerlig tilgang til informationssikkerhedskulturen har EasyIQ A/S et årligt IT-Sikkerhed informationsmøde. Informationen revurderes årligt af informationssikkerhedsorganisationen.

**Styring af it-sikkerhedshændelser**
Sikkerhedshændelser og svagheder i EasyIQ A/S systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt. Der er etableret procedurer for hændelsesstyring og afvigelsesrapportering, herunder sikkerhedsbrud. Procedurerne sikrer, at der arbejdes systematisk, foretages nødvendig dataindsamling og dokumentation, således at der efterfølgende er et godt grundlag at evaluere ud fra. Afvigerapporteringen er en del af vores Kvalitetsstyringssystem, og det Management, der er ansvarlig for at definere og koordinere en struktureret ledelsesproces, der sikrer en passende reaktion på sikkerhedshændelser.

**Brugerstyring/ adgangssikkerhed**
Den logiske sikring skal sikre, at kun autoriserede brugere har adgang til systemerne.
Tildeling af adgang til driftsmiljø skal ske i overensstemmelse med forretningsbetingede formål og informationernes klassifikation. Både fysisk og logisk adgang er baseret på principperne ”need-to-know” og ”least privillege”, hvor der tildeles adgang til de informationer, som man har behov for, for at kunne udføre sine opgaver/sit job eller rolle.

Anmodning om adgang til interne it-systemer og produktionsmiljøer følger en fastlagt procedure, der

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

sikrer en adskillelse i anmodning, godkendelse, verifikation og implementering. Adgangsstyringen dokumenteres i et centralt system.

Krav til password – alle brugere oprettet i EasyIQ A/S centrale brugerdatabase skal skifte password hver 90. dag. Passwordet skal være på mindst 8 tal eller bogstaver og indeholde special tegn, og de seneste 3 passwords kan ikke bruges igen.

Nye enheder (telefoner, routere, PC'ere) konfigureres og sættes op med nyt administratorpassword, forskellig fra default og enhederne krypteres.

Adgang til kildekode
For at forhindre uautoriseret funktionalitet eller andre skadelige ændringer er adgang til kildekode begrænset mest muligt.

**Fysisk sikkerhed**
EasyIQ A/S gør brug af eksterne leverandører til eksterne virksomhedens services:

- Fuzion - Stilling
- GlobalConnect - Hørning
- Microsoft Azure – Holland

Det betyder, at vi har overladt de grundlæggende datacenteropgaver til leverandøren, der er ekspert i opbygning og drift af datacentre.

Housing leverandørerne er ansvarlige for fysisk sikring, brand-, og vanddetektion og -bekæmpelse, strøm og køling. Housing leverandørernes datacentre giver flere lag sikkerhed og opfylder anerkendte internationale standarder for informationssikkerhed vedr. managementsystemer og business continuity management.

Dokumenterede driftsprocedurer
EasyIQ har indført driftsprocedurer, der sikrer, sikker drift af informationsbehandlingsfaciliteter. Driftsprocedurer gjort tilgængelige for relevante ansatte.

**Backup**
Formålet med backup er at sikre, at kundens data i EasyIQ A/S hostingcentre kan genskabes, nøjagtigt og hurtigt, så kunderne undgår unødvendig ventetid.
Der tages backup på forskellige niveauer som virtuelle servere, konfigurationer og data. Dette sikrer, at vi har flere muligheder for at sætte ind ved behov for reetablering. Der tages backup af relevante databaser og konfigurationer, med henblik på at muliggøre reetablering i en given nødsituation. Der er forskellige krav til frekvens af backups afhængigt af hvor kritisk it-systemet er. Backuppolitikken for databaser beskriver, at der skal tages daglige backups, minimum én i døgnet. For mindst én af disse backups foretages en reetableringstest, der tester backuppens integritet. Hver backup gemmes på dedikerede backupservere placeret i driftsmiljøet. Desuden flyttes backups til en fysisk adskilt lokation. Alle backups krypteres med AES-256 krypteringsnøgle, og transport af data mellem de 2 primær sites og foregår krypteret. Daglige database backups opbevares i 5 dage.

**Overvågning**
Driftsmiljøet overvåges 24/7/365 via en automatiseret service. Der overvåges ressourcer for servere (Cpu, ram, disk, netværk) og tilgængelighed. Overvågningen omfatter også relevante it-services eksempelvis backups, tilgængelighed for kundevendte systemer og systemer til internt brug. Den primære overvågning foregår internt i driftsmiljøet, men for også at dække den eksterne tilgængelighed har vi etableret en offsite overvågning. Ved fejl rapporteres til NOC, hvorefter fejlen bliver undersøgt. Er der tale om kritiske fejl i servere eller services, adviseres den vagthavende driftsmedarbejder direkte. Driftens NOC er til internt brug i EasyIQ A/S, og er således ikke tilgængelig for kunder. Kunder, Generelle

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

vilkår.

Beskyttelse af logoplysninger
Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang.

Driftsstatus kommunikeres via EasyIQ A/S hjemmeside: https://easyiq.dk/drift

**Patch management / ændringshåndtering**
Formålet med patch management er at sikre, at alle relevante opdateringer som patches, fixes og service packs fra leverandører implementeres for at sikre systemerne mod nedetid og uautoriseret adgang, og at implementeringen sker på en kontrolleret måde.
Vedligehold af Windows operativsystemer og tilhørende backend-systemer fra Microsoft, håndteres af Microsofts indbyggede WSUS (Windows Server Update Services), hvor sikkerheds- og kritiske patches installeres automatisk med faste intervaller.

Efter installation af operativsystemer følges en procedure, der sikrer, at det kun er relevante services og applikationer, der er tilgængelige på serveren.

Softwareinstallation i test- og produktionssystemer
EasyIQ 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.

EasyIQ har desuden opstillet generelle krav for installation af software på arbejdsstationer og servere.

**Kommunikationssikkerhed**
For at beskytte vores SaaS løsninger mod Cyberkriminalitet, har vi indført følgende systemer.
Alt internet trafik scannes og tjekkes med Cloudflare og Watchguard firewall's, dette indbefatter blandt andet DDoS beskyttelse og Intrusion Prevention Service (IPS) for at sikker at de data der hentes og sendes overholder gældende standard og ikke er fyldt med ondsindet data. Løsningen indeholder også load balancer funktionalitet for at sikre fordeling af trafik og oppetid, dette benyttes også i forbindelse med patch og opdateringer.

**Styring af it-sikkerhedshændelser**
Sikkerhedshændelser og svagheder i EasyIQ A/S systemer skal rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

Alle medarbejdere i EasyIQ A/S er bekendt med procedurerapportering af forskellige typer hændelser og svagheder, der kan have indflydelse på sikkerheden af EasyIQ A/S drift. Sikkerhedshændelser og svagheder skal hurtigst muligt rapporteres til direktionen.
Direktionen har ansvaret for at definere og koordinere en struktureret proces, der sikrer en passende reaktion på sikkerhedshændelser.

**Leverandørstyring**
Som leverandør til kritiske dele af vores driftsmiljø, fører EasyIQ A/S årligt kontrol med, om housing leverandørerne lever op til krav og SLA for deres ydelser. EasyIQ A/S evaluerer leverandørens certificeringer og sammenholder dem med egne observationer. Herefter vurderer vi, om leverandøren lever op til de aftalte serviceydelser, og hvorvidt der er grund til at tage aspekter op med dem.

**Beredskabsstyring**
EasyIQ A/S forretning er i stor grad baseret på den grundliggende it-infrastruktur, hvorfra it-services udbydes til kunderne. It-beredskabsplanen skal således ses som en samlet Business Continuity Plan (BCP) eller Forretningskontinuitetsplan.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

Ved alvorlige fejl informeres den it-sikkerhedsansvarlige og Management i EasyIQ A/S. Den aktuelle beredskabsplan beskriver, hvorledes der skal informeres, fejlsøges og fejlrettes. For at gøre planerne så operationelle som muligt er der etableret procedurer for beredskabsstyring på flere niveauer. En over ordnet BCP beskriver definitioner af beredskabsfaser, vurdering af hvor kritisk problemet er, eskalerings-, og kommunikationsprocedure. Planen beskriver håndteringen af to af de værst tænkelige scenarier: Nedbrud i datalinjer og totalt datacenternedbrud.

I løbet af kontrolperioden der udført en årlig kvalitetssikring af beredskabsplanen, hvorefter enkelte systemer vil bliveudvalgt til test.

**Ændringer i EasyIQ SaaS løsninger og de tilhørende generelle it-kontroller**
Der er i perioden fra 1. juli 2023 til 30. juni 2024 ikke foretaget væsentlige ændringer i ændringer i EasyIQ SaaS løsninger og de tilhørende generelle it-kontroller.

## KOMPLEMENTERENDE KONTROLLER HOS KUNDER AF EASYIQ SAAS LØSNINGER

Kunder af EasyIQ´ SaaS løsninger er forpligtet til at implementere følgende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for at opnå kontrolmålene:

- At sikre, at brugeroprettelser og brugersletning hos kunderne sker i deres eget studieadministrative system eller lønsystem, hvorefter der via en integration til Styrelsen for It og Læring sker adgangs- og rettighedstildeling i EasyIQ SaaS-løsninger. De dataansvarlige er derfor selv ansvarlige for, at deres brugere har de korrekte roller i eget studieadministrative system eller lønsystem.
- At sikre, at data er ajourførte og slettes behørigt, hvis det skal slettes tidligere end 90 dage efter brugerne er afmeldt.
- At sikre, at tilgang til terminaler, pc'ere, bærbare og andre enheder, der kan tilgå EasyIQ's Skoleportal og IT Platformen, alene sker for autoriserede brugere, herunder tildeling af rettigheder til autoriserede brugere.
- At sikre, at den kundens brugere er ajourførte.
- At sikre hensigtsmæssige kontroller for adgangsbrugeradministration og datamanagement, herunder sletning fra Windows Azure og Office 365 samt Googles G-suite.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

# 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 EasyIQ A/S' beskrivelse EasyIQ SaaS løsninger samt for udformningen og den operationelle effektivitet 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 eller ikke fungerer effektivt.

BDO's test af udformningen og den operationelle effektivitet af kontroller har omfattet de kontrolmål og tilknyttede kontrolaktiviteter, der er udvalgt af EasyIQ 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 og har fungeret effektivt i hele perioden fra 1. juli 2023 til 30. juni 2024.

### Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen og den operationelle effektivitet heraf er udført ved forespørgsel, inspektion, observation og genudførelse.

| Type | Beskrivelse |
|---|---|
| Forespørgsel | Forespørgsler hos EasyIQ A/S passende personale er udført for alle væsentlige kontrolaktiviteter.<br><br>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.<br><br>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. |
| Genudførelse | Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat. |

For de ydelser, som Microsoft Azure leverer inden for logning, har vi modtaget revisionserklæring for underserviceleverandørens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. oktober 2022 til den 30. september 2023, samt tilhørende bridgeletters.

For de ydelser, som Fuzion A/S leverer inden for housing af systemerne, har vi modtaget revisionserklæring for underserviceleverandørens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. juli 2022 til den 30. juni 2023.

For de ydelser, som GlobalConnect leverer inden for housing af systemerne, har vi modtaget revisionserklæring for underserviceleverandørens tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller for perioden 1. januar til den 31. december 2023.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

Disse serviceunderleverandøres relevante kontrolmål og tilknyttede kontroller indgår ikke i EasyIQ A/S' beskrivelse af EasyIQ SaaS løsninger og de tilhørende kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos EasyIQ A/S, der sikrer overvågning af serviceunderleverandørens opfyldelse af den mellem serviceunderleverandøren og EasyIQ A/S 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 og implementeret eller ikke har fungeret effektivt i perioden.

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## Risikovurdering

**Kontrolmål**

- *Risikovurdering skal identificere og prioritere risici med udgangspunkt i udviklingen og driften af SaaS løsninger. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Risikovurdering**<br><br>▶ Der foretages løbende og som minimum én gang årligt en risikovurdering af it-miljøerne baseret på potentielle risici for datas tilgængelighed, fortrolighed og integritet.<br>▶ Sårbarheden af systemer og processer vurderes ud fra identificerede trusler.<br>▶ Risici minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for risikovurdering, og observeret at den fastlægger at serviceleverandørens SaaS løsninger skal risikovurderes ud fra identificerede trusler og baseres på potentielle risici for datas tilgængelighed, samt at risici skal minimeres ud fra vurderingen af deres sandsynlighed, konsekvens og afledte implementeringsomkostninger.<br><br>Vi har inspiceret risikovurderingen af serviceleverandørens SaaS løsninger og observeret, at den er udarbejdet i overensstemmelse med proceduren.<br><br>Vi har inspiceret dokumentation for, at serviceleverandøren har foretaget den årlige gennemgang af risikovurderingen i erklæringsperioden.<br><br>Vi har observeret, at der ikke er sket ændringer i den vurdere risiko i erklæringsperioden. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.5 Informationssikkerhedspolitikker

**Kontrolmål**

- *Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Politikker for informationssikkerhed**<br><br>▶ Informationssikkerhedspolitikken og de tilhørende støttepolitikker er godkendt af virksomhedens direktion, og efterfølgende forankret ned gennem virksomhedens organisation. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og observeret, at denne tager udgangspunkt i ISO 27001 standarden.<br><br>Vi har inspiceret, at alle medarbejdere har underskrevet, at de har læst og accepteret informationssikkerhedspolitikken. | Ingen afvigelser konstateret. |
| **Gennemgang af politikker for informationssikkerhed**<br><br>▶ Informationssikkerhedspolitikken og de tilhørende støttepolitikker bliver gennemgået og opdateret minimum én gang årligt. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedspolitik og observeret, at det er direktørens ansvar at gennemgå og opdatere informationssikkerhedspolitikken minimum én gang årligt.<br><br>Vi har inspiceret, at direktøren har gennemgået informationssikkerhedspolitikken, og at denne er blevet godkendt af bestyrelsen i erklæringsperioden. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.6 Organisering af informationssikkerhed

**Kontrolmål**

- *Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikkerhedsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Roller og ansvarsområder for informationssikkerhed**<br><br>▶ Der er placeret et organisatorisk ansvar for it-sikkerhed, og det er dokumenteret og implementeret. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at direktøren har ansvaret for informationssikkerheden. | Ingen afvigelser konstateret. |
| **Politik for mobilt udstyr og fjernarbejdspladser**<br><br>▶ Risici i relation til anvendelse af mobilt udstyr og fjernarbejdspladser er identificeret, og sikkerhedsforhold i relation til anvendelsen er håndteret. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at serviceleverandøren har en politik for mobile enheder og fjernarbejdspladser, der fastlægger krav om anvendelse af Bitlocker, firewall og antivirus,<br><br>Vi har stikprøvevist inspiceret dokumentation for, at serviceleverandørens medarbejdere efterlever de angivne sikkerhedsforanstaltninger for mobile enheder. | Ingen afvigelser konstateret. |
| **Funktionsadskillelse**<br><br>▶ 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 forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret oversigt over fordeling af serviceleverandørens funktioner og ansvarsområder og observeret, at ansvarsområder er fordelt på forskellige afdelinger og personer. Vi har inspiceret dokumentation for at ansvarsopdelingen er etableret. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.6 Organisering af informationssikkerhed

**Kontrolmål**

- *Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikkerhedsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Informationssikkerhed ved brug af cloudtjenester**<br><br>▶ Serviceleverandøren har fastlagt, hvilke informationsrisici, der er forbundet ved anvendelse af Cloud-tjenester.<br>▶ Serviceleverandøren har processer for anskaffelse, brug, styring og afslutning af brugen af cloudtjenester i overensstemmelse med organisationens informationssikkerhedskrav. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for anvendelse af Cloud-tjenester og observeret, at der er fastlagt konkrete informationsrisici der skal overvejes ved anvendelse af Cloud-tjenester.<br><br>Vi har inspiceret serviceleverandørens procedure for anskaffelse, brug, styring og afslutning af brugen af cloudtjenester og observeret, at den er i overensstemmelse med organisationens informationssikkerhedskrav.<br><br>Vi har inspiceret dokumentation for, at serviceleverandøren har fulgt proceduren vedrørende brug og styring af Cloud-tjenester.<br><br>Vi er på forespørgsel blevet oplyst, at serviceleverandøren ikke har anskaffet nye Cloud-tjenester eller har ophørt eksisterende Cloud-tjenester i erklæringsperioden, hvorfor vi ikke har kunnet teste disse dele af procedurens implementering og effektivitet. | Vi har konstateret, at serviceleverandøren ikke har anskaffet nye Cloud-tjenester eller har ophørt eksisterende Cloud-tjenester i erklæringsperioden, hvorfor vi ikke har kunnet teste disse dele af procedurens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.7 Personalesikkerhed

**Kontrolmål**

- *Det skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Rekruttering af medarbejdere**<br><br>▶ Serviceleverandøren udfører baggrundstjek af alle jobkandidater i overensstemmelse med serviceleverandørens procedure og den funktion, som jobkandidaten skal besidde. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret, at serviceleverandørens procedure for rekruttering af medarbejdere og observeret, at der skal gennemføres baggrundstjek ved ansættelse af nye medarbejdere.<br><br>Vi har inspiceret dokumentation for, at der for alle nyansatte i erklæringsperioden er foretaget baggrundstjek i overensstemmelse med proceduren. | Ingen afvigelser konstateret. |
| **Under ansættelse**<br><br>▶ Serviceleverandøren afholder årligt et IT-sikkerhedsinformationsmøde for at sikre en kontinuerlig tilgang til informationssikkerhedskulturen.<br>▶ Alle medarbejdere har underskrevet en ansættelseskontrakt, der indeholder en bestemmelse om tavshedspligt. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at der skal afholdes et årligt møde til sikring af, at medarbejdere holdes ajour med sikkerhed og bevidstgøres om eventuelle nye trusler eller regler.<br><br>Vi har inspiceret dokumentation for at afholdelse af det årlige IT-sikkerhed informationsmøde og observeret, at alle medarbejdere har deltaget.<br><br>Vi har inspiceret serviceleverandørens skabelon til ansættelseskontrakter og observeret, at den indeholder bestemmelse om tavshedspligt.<br><br>Vi har inspiceret dokumentation for, at alle nyansatte i erklæringsperioden har underskrevet en ansættelseskontrakt, der er baseret på skabelonen og indeholder bestemmelse om tavshedspligt. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.7 Personalesikkerhed

**Kontrolmål**

- *Det skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Fratrædelse af medarbejdere**<br><br>▶ Serviceleverandøren har udarbejdet og implementeret en procedure for fratrædelse af medarbejdere ved ophør af ansættelse. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at når en medarbejder skifter ansvarsområde eller stopper i virksomheden, gennemgår og justerer lederen medarbejderens rettigheder og systemadgange.<br><br>Vi har observeret, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste for procedurens implementering og effektivitet. | Vi har konstateret, at der ikke været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.8 Styring af aktiver

**Kontrolmål**

- *Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig. Virksomheden skal sikre, at informationsaktiver får et passende beskyttelsesniveau.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Fortegnelse og ansvar og aktiver**<br><br>▶ Alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver.<br>▶ Der er udpeget en ejer for alle væsentlige aktiver i forbindelse med driften af SaaS løsninger. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret, at alle informationsaktiver er identificeret, og der er etableret en ajourført fortegnelse over alle væsentlige aktiver<br><br>Vi har observeret, at fortegnelsen er blevet opdateret i erklæringsperioden.<br><br>Vi har inspiceret, at serviceleverandøren har udpeget en ansvarlig for alle aktiver. | Ingen afvigelser konstateret. |
| **Klassifikation af information**<br><br>▶ Informationer og data i relation til SaaS løsninger og den efterfølgende drift af it-løsningerne er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret dokumentation for, at informationer og data i relation til SaaS løsninger og den efterfølgende drift af it-løsningerne er klassificeret på grundlag af forretningsmæssig værdi, følsomhed og behovet for fortrolighed. | Ingen afvigelser konstateret. |
| **Bortskaffelse af medier**<br><br>▶ Serviceleverandøren har udarbejdet og implementeret en procedure for bortskaffelse af medier, hvor der opbevares personoplysninger på forsvarlig vis. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret informationssikkerhedshåndbogen og observeret, at serviceleverandøren har en procedure, som skal sikre, at | Vi har konstateret, at der ikke har været medier eller udstyr, der er destrueret eller bortskaffet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.8 Styring af aktiver

**Kontrolmål**

- *Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og funktionsmæssige informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig. Virksomheden skal sikre, at informationsaktiver får et passende beskyttelsesniveau.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | medier/udstyr destrueres korrekt, således at data på medierne ikke kan genskabes.<br><br>Vi har observeret, at der ikke har været medier eller udstyr, der er destrueret eller bortskaffet i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet. | |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.9 Adgangsstyring

**Kontrolmål**

- *At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Politik for adgangsstyring**<br><br>▶ Der foreligger dokumenterede og ajourførte retningslinjer for serviceleverandørens adgangsstyring. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret, at der foreligger dokumenterede og ajourførte retningslinjer for serviceleverandørens adgangsstyring. | Ingen afvigelser konstateret. |
| **Brugerregistrering og -afmelding**<br><br>▶ Der er en formaliseret forretningsgang for tildeling og afbrydelse af brugeradgang. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for brugeradministration, som fastlægger, at brugeroprettelser og -nedlæggelser følger skal følge en styret proces, og at alle brugeroprettelser skal være autoriseret, og brugerrettigheder skal tildeles ud fra et arbejdsbetinget behov.<br><br>Vi har inspiceret dokumentation for, at alle brugeroprettelser i erklæringsperioden er sket i overensstemmelse med proceduren, og er autoriseret og at adgange er tildelt ud fra den ansattes arbejdsbetingede behov.<br><br>Vi har inspiceret dokumentation for, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste for procedurens implementering og effektivitet vedrørende nedlæggelser.<br><br>Vi har inspiceret, at kundens brugere automatisk oprettes og slettes gennem en integration til STIL, som trækker data fra kundens | Vi har konstateret, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunnet teste denne del af kontrollens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

| A.9 Adgangsstyring | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| | eget studieadministrative system. Kunderne er derfor selv ansvarlige for, at deres brugere har de korrekte roller i deres administrative system. | |
| **Styring af privilegerede adgangsrettigheder**<br><br>▶ Privilegerede (administrative) adgangsrettigheder tildeles til systemer og enheder ud fra arbejdsbetinget behov. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for brugeradministration, som fastlægger, at brugerrettighedsstyring skal følge en styret proces, og at brugerrettigheder skal tildeles ud fra et arbejdsbetinget behov.<br><br>Vi har på forespørgsel fået oplyst, at der ikke er tildelt privilegerede rettigheder til egne medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste for procedurens implementering og effektivitet.<br><br>Vi har inspiceret, at ved kundeoprettelse opretter serviceleverandøren den første privilegerede bruger til systemerne, som herefter kan tildele yderligere privilegerede rettigheder i deres organisation. | Vi har konstateret, at der ikke er tildelt privilegerede rettigheder til egne medarbejdere i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |
| **Gennemgang af brugeradgangsrettigheder**<br><br>▶ Interne brugeres adgangsrettigheder gennemgås regelmæssigt efter en formaliseret forretningsgang. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at der minimum én gang årligt skal foretaget periodisk gennemgang af brugere og tilhørende rettigheder. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.9 Adgangsstyring

**Kontrolmål**

- *At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | Vi har inspiceret, at serviceleverandøren har gennemgået brugere og tilhørende rettigheder i erklæringsperioden. | |
| **Procedurer for sikkert log-on**<br><br>- Serviceleverandøren har etableret logisk adgangskontrol til systemer med personoplysninger, som skal følges af alle medarbejdere | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret passwordpolitikken til serviceleverandørens SaaS løsninger samt medarbejdernes arbejdscomputere og observeret, at serviceleverandøren har etableret tilstrækkelig logisk adgangskontrol til systemer og arbejdscomputere. | Ingen afvigelser konstateret. |
| **Adgang til kildekode**<br><br>- For at forhindre uautoriseret funktionalitet eller andre skadelige ændringer er adgang til kildekode begrænset mest muligt. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for adgang til kildekode og observeret, at adgang til kildekoden skal begrænses.<br><br>Vi har inspiceret dokumentation for, at adgang til kildekoden er begrænset. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.12 Driftssikkerhed

**Kontrolmål**

- *En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Dokumenterede driftsprocedurer**<br><br>▶ Der er indført driftsprocedurer, der sikrer, sikker drift af informationsbehandlingsfaciliteter. Driftsprocedurer gjort tilgængelige for relevante ansatte. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens driftsprocedure og observeret, at de omhandler sikker drift af informationsbehandlingsfaciliteter og er tilgængelig for alle ansatte. | Ingen afvigelser konstateret. |
| **Vedligeholdelse af systemsoftware**<br><br>▶ Operativsystem-software på servere og arbejdsstationer opdateres løbende. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har på forespørgsel fået oplyst, at serviceleverandørens medarbejdere selv er ansvarlige for at opdatere deres arbejdscomputere.<br><br>Vi har stikprøvevist inspiceret dokumentation for, at serviceleverandørens medarbejdere har opdateret deres operativsystemsoftware.<br><br>Vi har inspiceret serviceleverandørens procedure for vedligeholdelse af servere og observeret, at opdatering af servernes operativsystem skal ske løbende og minimum hvert kvartal.<br><br>Vi har stikprøvevist inspiceret, at serveres operativsystem-software er opdateret. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.12 Driftssikkerhed

**Kontrolmål**

- *En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | | |
| **Antivirusprogram**<br><br>▶ Der er installeret antivirus-software på alle servere og arbejdsstationer.<br>▶ Antivirus-software opdateres løbende til seneste version. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at den fastlægger at servere og arbejdsstationer skal have installeret opdateret antivirus.<br><br>Vi har stikprøvevist inspiceret, at serviceleverandørens medarbejdere har installeret og opdateret antivirus på deres arbejdscomputere.<br><br>Vi har stikprøvevist inspiceret, at servere har installeret og opdateret antivirus. | Ingen afvigelser konstateret. |
| **Sikkerhedskopiering og retablering af data**<br><br>▶ Generel OS Backup – foretages 1 gang pr. uge og gemmes i 4 uger<br>▶ Kritiske OS Backup - backup hver dag og gemmes i 4 uger<br>▶ SQL Backup – Backup hver dag og gemmes i 14 dage<br>▶ Der udføres restore-tests én gang årligt. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret procedure for backup og observeret, at der skal foretages general OS backup 1 gang pr. uge, som gemmes i 4 uger, at der for kritiske OS-backup foretages daglig backup, som gemmes i 4 uger og at der skal foretages SQL backup dagligt, som gemmes i 14 dage. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.12 Driftssikkerhed

**Kontrolmål**

- *En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | Vi har inspiceret, at serviceleverandøren foretager backup i overensstemmelse med serviceleverandørens procedure.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at der er beskrevet krav om restore-test minimum én gang årligt.<br><br>Vi har inspiceret, at der er gennemført restore-test i erklæringsperioden. | |
| **Logning i systemer, databaser og netværk, herunder logning af anvendelse af personoplysninger**<br><br>- Der anvendes et centralt overvågningsværktøj, der afgiver alarmer, hvis kendte fejl opstår.<br>- Alle succesfulde adgange og mislykkede adgangsforsøg til serviceleverandørens systemer og data logges.<br>- Alle brugerændringer i system og databaser logges.<br>- Loggen slettes efter den fastsatte retentionsperiode, som serviceleverandøren monitorerer og logger netværkstrafik. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens overvågningsværktøj og observeret, at der overvåges for fejl og udsendes alarmer herom.<br><br>Vi har stikprøvevist inspiceret hændelseslog for serviceleverandørens systemer og data og observeret at alle succesfulde adgange og mislykkede adgangsforsøg, samt brugerændringer, logges.<br><br>Vi har inspiceret dokumentation for, at logs ikke opbevares i længere tid end den fastsatte retentionperiode. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.12 Driftssikkerhed

**Kontrolmål**

- *En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Beskyttelse af logoplysninger**<br><br>▶ Logningsfaciliteter og logoplysninger skal beskyttes mod manipulation og uautoriseret adgang. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har foretaget inspektion af dokumentation, der sikrer at logningsfaciliteter og logoplysninger er beskyttet mod manipulation og uautoriseret adgang. | Ingen afvigelser konstateret. |
| **Overvågning**<br><br>▶ Serviceleverandøren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet.<br>▶ Serviceleverandøren notificeres om identificerede alarmer og følger op herpå. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret, at serviceleverandøren har etableret et overvågningssystem til overvågning af produktionsmiljø, herunder oppetid, ydeevne og kapacitet.<br><br>Vi har inspiceret, at serviceleverandøren notificeres om identificerede alarmer. | Ingen afvigelser konstateret. |
| **Softwareinstallation i test- og produktionssystemer**<br><br>▶ Der er 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.<br>▶ Serviceleverandøren har opstillet generelle krav for installation af software på servere. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.12 Driftssikkerhed

**Kontrolmål**

- *En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter, og de heraf afledte kapacitetskrav.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At sikre den ønskede tilgængelighed til virksomhedens informationsaktiver. Der skal være etableret faste procedurer for sikkerhedskopiering og løbende afprøvning af kopiernes anvendelighed.*
- *At afsløre uautoriserede handlinger. Forretningskritiske it-systemer skal overvåges og sikkerhedsrelaterede hændelser skal registreres. Der skal være en logning, som sikrer, at uønskede forhold konstateres.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| ▶ Serviceleverandøren har procedure for installation af software på arbejdsstationer | Vi har inspiceret serviceleverandørens generelle krav til installation af software på servere.<br><br>Vi har inspiceret serviceleverandørens procedure for installation af software på arbejdsstationer.<br><br>Vi har inspiceret at serviceleverandøren automatisk alarmeres ved installation af uautoriseret software på servere. | |
| **Sårbarhedsscanning**<br><br>▶ Der foretages løbende sårbarhedsscanning af serviceleverandørens netværk. Resultatet dokumenteres i en rapport.<br>▶ Serviceleverandøren gennemgår rapporten og følger op på konstaterede svagheder.<br>▶ Serviceleverandøren håndterer/mitigerer eventuelle sårbarheder ud fra en risikovurdering.<br>▶ Serviceleverandøren har dokumenteret deres håndtering/mitigering af fundne sårbarheder. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret procedure for gennemførsel af løbende sårbarhedsscanninger og observeret, at serviceleverandørens direktør hver måned modtager en rapport på baggrund af seneste måneds scanninger.<br><br>Vi har inspiceret dokumentation for gennemførte sårbarhedsscanninger og observeret, at der ikke er konstateret nogle svagheder af høj risiko.<br><br>Vi er på forespørgsel blevet oplyst, at der ikke har været nødvendigt at implementere mitigerende foranstaltninger på baggrund af udførte sårbarhedsscanninger i erklæringsperioden. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

| A.13 Kommunikationssikkerhed | | |
|---|---|---|
| **Kontrolmål**<br>▶ *At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.* | | |
| **Kontrolaktivitet** | **Test udført af BDO** | **Resultat af test** |
| **Netværkssikkerhed**<br><br>▶ Netværkstopologien er struktureret efter best-practice principper, hvilket betyder at servere, som driver applikationer, ikke kan nås direkte fra internettet. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens netværkstypologi og observeret, at al kundetrafik køres gennem Cloudflare for filtrering og DDoS beskyttelse, hvilket sikrer at servere, som driver applikationer, ikke kan nås direkte fra internettet.<br><br>Vi har inspiceret, at netværksfirewall er opsat, således at servere, som driver applikationer, ikke kan nås direkte fra internettet. | Ingen afvigelser konstateret. |
| **Firewall**<br><br>▶ Serviceleverandøren har konfigureret firewall efter minimumsprincippet.<br>▶ Arbejdsstationer benytter firewall. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for håndtering af netværkssikkerhed og observeret, at alene godkendt netværkstrafik må komme gennem firewallen.<br><br>Vi har stikprøvevist inspiceret opsætning af firewall på servere og observeret, at alene godkendt netværkstrafik kan komme gennem firewallen.<br><br>Vi har inspiceret serviceleverandørens informationssikkerhedshåndbog og observeret, at alle serverer og arbejdsstationer skal benytte firewall.<br><br>Vi har stikprøvevist inspiceret dokumentation for, at firewall er aktiveret på arbejdsstationer og servere. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

**Kontrolmål**

- *At sikre, at Informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Sikker udviklingspolitik**<br><br>▶ Serviceleverandøren har tilrettet systemudvikling og vedligeholdelsesaktiviteter baseret på en egenudviklet projektmodel.<br>▶ Alle ændringer, som skal idriftsættes i produktionsmiljøet, skal være godkendt før udrulning.<br>▶ Der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for ændringsstyring og observeret, at:<br>▶ Alle ændringer drøftes, prioriteres og godkendes af ansvarshavende<br>▶ Alle ændringer testes<br>▶ Alle ændringer godkendes før idriftsættelse<br><br>Vi har inspiceret, at serviceleverandøren har fulgt processen for udvikling og vedligeholdelse af systemer.<br><br>Vi har inspiceret, at der benyttes et versionsstyringssystem, som registrerer alle ændringer i kildekode. | Ingen afvigelser konstateret. |
| **Adskillelse af udviklings-, test- og produktionsmiljø**<br><br>▶ Udviklings-, test- og produktionsmiljøer er adskilt. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har fået fremvist og inspiceret, at udvikling og test udføres i miljøer, som er adskilt fra produktionsmiljøet. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.15 Leverandørforhold

**Kontrolmål**

- *Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Håndtering af sikkerhed i leverandøraftaler**<br><br>▶ Risici i relation til eksterne parter er identificeret, og sikkerhed i aftaler med tredjemand og sikkerhedsforhold i relation til leverandører håndteres. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret indgået aftaler med eksterne leverandører og observeret, at der er indgået krav om sikkerhed. | Ingen afvigelser konstateret. |
| **Styring af ændringer af leverandørydelser.**<br><br>▶ Ved ændringer, der påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden. Der anvendes udelukkende anerkendte leverandører. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for, at der ved ændringer, som påvirker produktionsmiljøet, og hvor der anvendes service fra eksterne leverandører, bliver disse udvalgt af den ansvarlige for it-sikkerheden.<br><br>Vi har på forespørgsel fået oplyst, at der ikke er sket ændringer i brugen af eksterne leverandører i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet. | Vi har konstateret, at der ikke er sket ændringer i brugen af underserviceleverandører i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |
| **Overvågning og gennemgang af leverandørydelser**<br><br>▶ Der føres tilsyn med eksterne samarbejdspartnere. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret serviceleverandørens procedure for overvågning og tilsyn med eksterne leverandører.<br><br>Vi har inspiceret, at serviceleverandøren har gennemført tilsyn med eksterne leverandører i erklæringsperioden. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.15 Leverandørforhold

**Kontrolmål**

- *Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| | Vi har inspiceret seneste 3402 erklæring fra Fuzion for perioden 1. juli 2022 til 30. juni 2023.<br><br>Vi har inspiceret seneste 3402 erklæring fra GlobalConnect for perioden 1. januar til 31. december 2023.<br><br>Vi har inspiceret seneste SOC 2 erklæring fra Microsoft Azure for perioden 1. oktober, 2022 – 30. september 2023 og tilhørende bridge letters.<br><br>Vi har inspiceret, at serviceleverandøren har gennemgået revisionserklæringerne og observeret, at de er vurderet tilstrækkelige og tilfredsstillende. | |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.16 Styring af informationssikkerhedsbrud

**Kontrolmål**

- *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Ansvar og procedurer**<br><br>▶ Der er fastlagt ledelsesansvar og roller i forbindelse med informationssikkerhedsbrud.<br>▶ Serviceleverandøren har implementeret procedure for brud på informationssikkerhedsbrud. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret, at serviceleverandøren har en procedure for håndtering af informationssikkerhedsbrud og observeret, at der er fastlagt ledelsesansvar og roller i forbindelse med brud på informationssikkerheden.<br><br>Vi er på forespørgsel blevet oplyst, at der ikke er konstateret brud på persondatasikkerheden i erklæringsperioden, hvorfor vi ikke har kunnet teste procedurens implementering og effektivitet. | Vi har konstateret, at der ikke har været brud på persondatasikkerhed i erklæringsperioden, hvorfor vi ikke har kunnet teste kontrollens implementering og effektivitet.<br><br>Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

## A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

**Kontrolmål**

- *Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering.*

| Kontrolaktivitet | Test udført af BDO | Resultat af test |
|---|---|---|
| **Beredskabsplaner i tilfælde af fysisk eller teknisk hændelse**<br><br>▶ Serviceleverandøren har etableret en beredskabsplan, der sikrer hurtig responstid til rettidig at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.<br>▶ Serviceleverandøren har etableret periodisk afprøvning af beredskabsplanen med henblik på at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer. | Vi har udført forespørgsel hos passende personale hos serviceleverandøren.<br><br>Vi har inspiceret, at serviceleverandøren har en beredskabsplan for, at sikrer hurtig responstid til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse.<br><br>Vi har inspiceret, at serviceleverandøren har gennemført test af beredskabsplanen i erklæringsperioden. | Ingen afvigelser konstateret. |

Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ

**BDO STATSAUTORISERET REVISIONSAKTIESELSKAB**

**VESTRE RINGGADE 28**
**8000 AARHUS C**

www.bdo.dk

*BDO Statsautoriseret revisionsaktieselskab, danskejet rådgivnings- og revisionsvirksomhed, er medlem af BDO International Limited - et UK-baseret selskab med begrænset hæftelse - og del af det internationale BDO-netværk bestående af uafhængige medlems-firmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.700 medarbejdere, mens det verdensomspændende BDO-netværk har over 115.000 medarbejdere i 166 lande.*

*Copyright - BDO Statsautoriseret revisionsaktieselskab, cvr.nr. 20 22 26 70.*

*Penneo dokumentnøgle: DHD0U-N25T2-LNXH8-VNOBV-T0YN6-WE2AZ*