FUZION A/S

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JULI 2022 TIL 30. JUNI 2023 OM BESKRIVELSEN AF DATACENTER-LØSNING OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING 2

2. FUZION A/S' UDTALELSE 4

3. FUZION A/S' BESKRIVELSE 5

Indledning 5

Beskrivelse af Fuzion 5

Fuzions co-location services 5

Forretningsstrategi/it-sikkerhedsstrategi 6

Risikostyring i Fuzion 6

Informationssikkerhedspolitikker 7

Organisering af Informationssikkerhed 7

Medarbejdersikkerhed 7

Fysisk sikring og miljøsikring 7

Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring 9

Ændringer i perioden fra 1. juli 2022 til 30 juni 2023 9

4. KONTROLMÅL, KONTROLAKTIVITETER, TEST OG RESULTAT AF TEST 10

A.5 – Informationssikkerhedspolitikker 11

A.6 - Organisering af informationssikkerhed 12

A.7 – Medarbejdersikkerhed 13

A.11 - Fysisk sikring og miljøsikring 16

A.17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring 21

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JULI 2022 TIL 30. JUNI 2023 OM BESKRIVELSEN AF DATACENTER-LØSNING OG DE TILHØRENDE KONTROLLER OG DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

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

Omfang

Vi har fået som opgave at afgive erklæring om den af Fuzion A/S (serviceleverandøren) for hele perioden fra 1. juli 2022 til 30. juni 2023 udarbejdede beskrivelse i sektion 3 af datacenter-løsning 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 risiciene 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

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

kontrolmål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet i sektion 2.
Det er vores opfattelse, at det opnåede bevis er tilstrækkeligt og egnet til at danne grundlag for vores konklusion.

Begrænsninger i kontroller hos en serviceleverandør

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 datacenter-løsning, 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 datacenter-løsning og de tilhørende kontroller, således som de var udformet og implementeret i hele perioden fra 1. juli 2022 til 30. juni 2023, 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 2022 til 30. juni 2023, 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 1. juli 2022 til 30. juni 2023.

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 datacenter-løsning, 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 10. juli 2023

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, statsautoriseret revisor

Mikkel Jon Larssen
Partner, chef for Risk Assurance, CISA, CRISC

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

2. FUZION A/S' UDTALELSE

Fuzion har til opgave at levere co-location datacenter-løsning selskabets kunder omkring drift, infrastruktur og processer.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt datacenter-løsningen, 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.

Fuzion A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af datacenter-løsning og de tilhørende kontroller i hele perioden fra 1. juli 2022 til 30. juni 2023. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for datacenter-løsning, og hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser, der er leveret i forbindelse med datacenter-løsning.
    - De processer i både it- og manuelle systemer, der er anvendt til styring af kontrolmiljøet.
    - Relevante kontrolmål og kontroller, der er udformet for at nå disse mål.
    - Andre aspekter ved vores kontrolmiljø, risikovurderingsproces, informationssystem (herunder de tilknyttede forretningsgange) og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for kundernes datacenter-løsning.
2. Indeholder relevante oplysninger om ændringer i serviceleverandørens datacenter-løsningen foretaget i perioden 1. juli 2022 til 30. juni 2023.
3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af Datacenter-løsning 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 datacenter-løsning, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

Fuzion 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 2022 til 30. juni 2023. 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.
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 2022 til 30. juni 2023.

Skanderborg, den 10. juli 2023

Fuzion A/S

Christian Holm Christensen
Adm. direktør

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

3. FUZION A/S' BESKRIVELSE

Indledning

Fuzion har til opgave at levere information til selskabets kunder samt revisorer omkring drift, infrastruktur og processer. Vi har også leveret denne information til vores egen eksterne revisor med henblik på at opnå denne ISAE 3402-2-erklæring, som er den internationale revisionsstandard for kontroller hos en serviceleverandør.

Beskrivelsen forventes også anvendt af Fuzions kunder, der arbejder med ISO 27001. Derfor er beskrivelsen af tekniske og organisatoriske sikkerhedsforanstaltninger formuleret og struktureret efter kontrollerne i ISO 27002, der i tillæg til 27001 indeholder retningslinjer for, hvordan man skal implementere kontroller nævnt i Annex A i ISO 27001.

Beskrivelsen kan anvendes af en kunde til at påvise, at kunden har passende tekniske og organisatoriske sikkerhedsforanstaltninger for deres behandling af personoplysninger (GDPR). Det er vigtigt i denne sammenhæng at præcisere, at Fuzion i GDPR-regi ikke er databehandler for de personoplysninger, som Fuzions kunder måtte indehave på udstyr opstillet i Fuzions datacentre.

Beskrivelsen er udarbejdet for at opfylde de typiske behov hos en bred kreds af kunder og deres revisorer, og den vil derfor ikke omfatte ethvert aspekt, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

Denne beskrivelse omfatter de kontrolaspekter, som er relevante for co-location og som relaterer sig til fysisk sikkerhed, risikostyring og beredskab. Der har ikke været væsentlige ændringer i Fuzions procedurer og kontrolmiljø i perioden 1. juli 2022 til 30. juni 2023.

Beskrivelse af Fuzion

Fuzion er startet i 2001 og servicerer i dag over 100 kunder fra ind- og udland. Fuzions har løbende bygget og udvidet datacenterforretningen. Først med et datacenter i Aarhus og siden med datacenter i Skanderborg og i 2019 med et supplerende datacenter i Randers. I 2021 er endnu et datacenter kommet til i Viby J. Fuzion er med sine fire lokationer en førende udbyder af datacenter faciliteter i det vestlige Danmark.

Fuzion blev i 2010 solgt til Nianet og skiftede i den forbindelse navn til Nianet. Fra 2010 til 2018 var Fuzion ejet af Nianet indtil selskabets to datacentre i hhv. Skanderborg og Aarhus i 2018 blev solgt til private danske investorer. I den forbindelse blev navnet Fuzion genindført, idet selskabet hele tiden havde været aktivt som selskab under Nianet.

Fuzion leverer datacenterinfrastruktur til kunder med forretningskritiske it-systemer. Fuzion har små og store kunder, private og offentlige. Fælles for dem er ønsket om et professionelt it-miljø til deres forretning, infrastruktur og applikationer. Mange af kunderne lever af deres it-infrastruktur ved for eksempel at levere cloud, hosting, online applikationer og internetløsninger til andre kunder.

Fuzions co-location services

Fuzions datacentre er designet og bygget efter anerkendte internationale standarder for sikre datacentre og er løbende moderniseret, udvidet og effektiviseret med de nyeste løsninger inden for "Datacenter Infrastruktur Management" til overvågning og proaktive meldesystemer.

Fuzions datacentre er designet til co-location, hvilket betyder, at de er de bygget til at servicere et større antal kunder med høj grad af fleksibilitet og sikker adskillelse af kundernes infrastruktur.

Fuzion er carrier- og operatørneutral, hvilket betyder, at kunder frit vælger leverandør af datalinjer og internet samt partnere til driftssamarbejde.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

Fuzion tilbyder assistance til kunder i datacentrene, så kunderne ikke selv behøver at møde op i datacentret for at installere servere, genstarte udstyr, tjekke kabling eller andre dele af deres installation. Fuzion tilbyder også rådgivning om, hvordan man får den bedste udnyttelse af selskabets co-location faciliteter med henblik på fx strømkabling, køling i rackskabet m.v.

Mange kunder bruger flere af Fuzions datacentre, da brugen af de flere datacentre giver øget redundans og dermed større sikkerhed for data og oppetid. Fuzions datacentre tilbyder samtidigt en geografisk afstand mellem centrene der sikrer mod at lokale uheld rammer flere Fuzion datacentre på samme tid, men også en afstand som kunderne finder rimelig, når man skal køre til flere centre for at sikre driften. På den måde kan Fuzion servicere kunder fra det meste af Jylland.

Hertil kommer at Fuzions datacenter i Randers er det nordligste carrier neutrale co-location datacenter i Jylland – sammenholdt med tilsvarende udbydere, der normalt betragtes som co-location udbydere på det jyske marked.

Forretningsstrategi/it-sikkerhedsstrategi

Fuzion arbejder efter en vision om at gøre markedet for datacentre mere grønt og fleksibelt. Den vision skal nås gennem vækst, hvor Fuzion leverer energieffektive og sikre datacenterløsninger til et stigende antal kunders kritiske infrastruktur som private og offentlige cloud-løsninger, Internet of Things (IOT), online apps, internet og meget mere – nu og i fremtiden.

Fuzion har en klar strategi om at opnå vækst ved at møde kunderne med ledig kapacitet, fleksible co-location-løsninger med høj kvalitet til en fornuftig pris og med en god service og meget høj integritet i forhold til kvalitet, test, drift, vedligehold, dokumentation og kommunikation med kunderne.

Fusions forretning er at levere den nødvendige fysiske sikkerhed og oppetid for den infrastruktur, som Fuzions kunder installerer og drifter i rackskabe, som kunderne har lejet i Fuzions datacentre.

Fuzions kerneforretning inden for co-location services er at levere:

- Høj oppetid på strøm leveret med UPS og generator backup
- Effektiv køling af infrastruktur til enhver tid
- Sikre adgangsforhold, som giver kunder fleksibel adgang og holder andre ude
- Et rent og brugervenligt arbejdsmiljø for it-udstyr og mennesker
- God kundeservice med hurtig og fleksibel leverance.

Fuzion skal sikre kundernes infrastruktur med et effektivt værn mod sikkerhedsmæssige trusler. Beskyttelsen er vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Såvel ansatte, gæster, kunder og eksterne personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe er hævet over sikkerhedsbestemmelserne.

Fuzions sikkerhedskoncept er organiseret omkring et Årshjul, der omfatter løbende vedligehold, eftersyn og opdatering af risikovurderinger, beredskabsplaner og sikkerhedsdokumentation.

Risikostyring i Fuzion

Ansvaret for risikostyringen ligger hos den administrerende direktør og udføres i tæt samarbejde med Site Manageren.

Fuzion forbedrer løbende sikkerheden. Der gennemføres årligt en formaliseret risikovurdering for at sikre, at sikkerhedsforanstaltningerne er tilstrækkelige, dokumenterede og godkendt af ledelsen.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

Fusion anvender i forbindelse med risikovurderingen blandt andet:

- Uptime Institutes anbefalinger - for at vurdere og sikre oppetider
- ASHRAE's anbefalinger for energieffektiv klimakontrol i datacentre
- Forsikringsselskabernes modeller til vurdering af indbrudssikring.

Informationssikkerhedspolitikker

Fuzion har med udgangspunkt i en risikovurdering udarbejdet en informationssikkerhedspolitik, der gennemgås og godkendes af ledelsen minimum én gang årligt.

Der er etableret processor til sikring af, at politikker kommunikeres til medarbejdere og relevante eksterne parter.

Organisering af Informationssikkerhed

Den overordnede ansvarlige for forretningen og sikkerheden er den administrerende direktør, som arbejder tæt sammen med den teknisk ansvarlige Site Manager. Site Manageren er ansvarlig for den daglige drift.

Ansvaret for de specifikke sikkerhedsforanstaltninger fremgår af Fuzions sikkerhedspolitik.

Medarbejdersikkerhed

Fuzions har etableret en intern proces for ansættelse, der sikrer at medarbejdere interviewes og kontrolleres, så der opnås sikkerhed om straffeattest, uddannelsespapirer, kørekort, erfaring og om nødvendigt referencer. Ansættelseskontrakten indeholder en tavshedsklausul og en sanktionsproces, i tilfælde af medarbejdere der begår informationssikkerhedsbrud. Der er ligeledes etableret en procedure til sikring af, at medarbejdere gøres opmærksomme på, at tavshedsklausulen fortsat er gældende efter ansættelsesforholdets ophør eller ændring.

Der afholdes årlige medarbejderudviklingssamtaler med medarbejdere for at sikre, at medarbejderne har de fornødne kompetencer og uddannelser for at varetage deres funktion. Ledelsens sikrer ligeledes, at medarbejdere holdes ajour med relevante sikkerhedskrav og pligter.

Fysisk sikring og miljøsikring

Sikkerhed, fysisk adgang

Fuzion har etableret formelle politikker og procedurer for kontrol af adgang til systemer, faciliteter og datacentre. Disse politikker og procedurer definerer den adgang, der er tilladt for kunder, medarbejder, gæster og håndværkere, og beskriver de tiltag og tilladelser, der kræves for at opnå og overvåge adgang.

Adgang foregår blandt andet via sluser med dobbelte døre, for at sikre adgangen og identiteten på de besøgende. Sluserne giver en ekstra skalsikring og sikrer mod, at uønskede gæster kan løbe med ind, når døren åbnes.

Adgangssystemer er basereret på multifaktor teknologi med en kombination af kort, kode og nøgler.

Fuzions husregler fremgår af skilte ved indgangen.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

Sikkerhedsforanstaltninger adgang og overvågning

Der foreligger forretningsgange og arbejds- og kontrolbeskrivelser på væsentlige og kritiske områder vedrørende fysisk sikkerhed.

Fysisk adgangskontrol

Adgangen til datacentre administreres udelukkende af Fuzion. Kunder skal indsende anmodning for at få udstedt kort, som kan give adgang for medarbejdere. Kunder skal også anmode om tilladelse til at ledsage gæster til datacentrene.

Der udstedes personlige adgangskort med foto samt tilhørende personlig adgangskode. Kunder har udelukkende adgang til de områder, som de skal igennem for at komme til deres egne aflåste rackskabe.

Datacenterindgange er sikret af elektroniske læsere af adgangskort, som er forbundet med en central computer, som giver og registrer al adgang til datacentrene.

Der er etableret procedurer, som sikrer at adgangsrettigheder opdateres og adgangskort lukkes for medarbejdere og eksterne brugere, hvis disse f.eks. har fratrådt deres stilling.

Overvågning

Fuzions datacentre er udvendigt og indvendigt udstyret med overvågningskameraer – CCTV – som er forbundet med en 24/7 bemandet vagtcentral. Alle døre til datacentrene er udstyret med alarmer og overvåges med videokameraer. Videoaktivitet overføres til en central server. Sikkerhedspersonalet følger med på videoovervågningen, hvis døralarmer eller andre alarmer aktiveres. Sikkerhedsvagter konfronterer alle uautoriserede eller mistænkelige personer, som forsøger at få adgang. Derudover er al adgang til datacentre overvåget, således, at kontrolleret/autoriseret adgang opretholdes.

Sikring af infrastruktur og drift

Fuzions datacentre er designet, bygget og driftes i henhold til internationalt anerkendte standarder for datacentre fra blandt andet (Uptime Institute og ASHRAE) og Fuzion kan levere datacenter/co-location service på Tier 2/3 niveau.

Strøm

Strømforsyning leveres via separate transformerstationer og ledningsføringsveje. Fuzion har standby-generatorer og redundant UPS-anlæg, som sikrer stabil elforsyning ved nedbrud på offentlig forsyning. Generatorerne og UPS testes og vedligeholdes regelmæssigt i henhold til Fuzions Årshjul og producenternes specifikationer.

Køling

Køling af rackskabe i datacentre leveres med blandt andet med down flow units, der sender kold og filtreret luft under hævede edb-gulve frem til kulde kuber, som holder den varme og kolde luft adskilt. I nogle af Fuzions serverrum bruges der inrow køling, som fungerer med enten kolde eller varme gange, hvor varmen fra serverne tvinges ud gennem inrows, som i den proces køler luften til det åbne areal, hvorfra infrastrukturen køles. Fuzions downflow og inrow får kølevand fra udendørs enheder, der køler vandet med en kombination af frikøl og kompressorkøl. I alle områder kontrolleres og styres temperaturen gennem overvågningsenheder med alarmer på.

Brandsikring og slukning

Datacentrene er opført i brandhæmmende materiale og beskyttet af automatiske brandslukningsanlæg, der er koblet til røgalarmer placeret i loftet og under de hævede gulve i server- og infrastrukturrum. Røgalarmerne suger konstant luft ind og analyserer på partikler for at kunne levere en meget tidlig audiovisuel alarm, hvis grænseværdier overskrides samt udløse brandslukning, når det behøves. Dette system kendes også som et VESDA-system – Very Early Smoke Detecting Apparatus.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

Brandslukning foretages med blandt andet med Inergen, der kvæler ild, og den begrænses til de rum, hvor alarmsystemerne registrer røgudvikling og der sendes samtidig alarm videre til kontrolcentralen.

Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring

Fuzion har etableret en beredskabsplan, der løbende opdateres og sikrer, at co-location services genetableres hurtigst muligt i tilfælde af en hændelse og at omfanget af skader på mennesker, faciliteter og kunders udstyr begrænses. Beredskabsplanen gennemgås minimum én gang årligt, for at sikre, at beredskabsplanen er tidssvarende og effektiv i kritiske situationer.

Der gennemføres årligt en test af beredskabsplanen.

Ændringer i perioden fra 1. juli 2022 til 30 juni 2023

Fuzion har ikke foretages væsentlige ændringer i de etablerede kontroller eller tekniske sikringsforanstaltninger i perioden i perioden 1. juli 2022 til 30 april 2023.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

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 Fuzion A/S' beskrivelse datacenter-løsning 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 Fuzion 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 2022 til 30. juni 2023.

Udførte testhandlinger

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

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.
Genudførelse	Kontroller er genudført for at verificere, at kontrollen fungerer som forudsat.

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: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.5 - Informationssikkerhedspolitikker		
Kontrolmål ▶ *At give retningslinjer for og understøtte Informationssikkerhed i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter. DS/ISO IEC 27002:2017*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
A.5.1.1: Politiker for risikostyring og Informationssikkerhed ▶ Ledelsen gennemfører en årlig risikovurdering, der giver grundlag for implementering af sikkerhedskrav i infrastruktur som varetages af Fuzion. ▶ Ledelse fastlægger og godkender informationssikkerhedspolitik og tilhørende sikkerhedsregler ▶ Ledelsen skal sikre at alle medarbejdere bliver bekendt med informationssikkerhedspolitikken ved ansættelse og gennem løbende vedligeholdelse.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret, at serviceleverandørens risikovurdering er godkendt af ledelsen i erklæringsperioden. Vi har inspiceret, at der foreligger en ledelsesgodkendt it-sikkerhedspolitik. Sikkerhedspolitikken er senest revurderet i 2021. Det er oplyst, at der ikke har være ændringer til sikkerhedspolitikken i erklæringsperioden. Vi har inspiceret, at ledelsen sikrer, at medarbejderne bliver gjort bekendt med informationssikkerhedspolitikken. Vi har inspiceret dokumentation for, at medarbejdere har læst og forstået fastsatte sikkerhedskrav.	Ingen afvigelser konstateret.
A.5.1.2: Gennemgang af politikkerne for Informationssikkerhed ▶ Ledelsen revurderer årligt Informationssikkerhedspolitikken og andre politikker og procedurer for informationsstikkerhed.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret, at serviceleverandørens informationssikkerhedspolitik er revurderet i erklæringsperioden i overensstemmelse med serviceleverandørens årshjul. Vi har på forespørgsel fået oplyst, at der ikke er foretaget væsentlige ændringer i politikkerne for Informationssikkerhed i erklæringsperioden.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.6 - Organisering af informationssikkerhed

Kontrolmål

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af Informationssikkerhed i organisationen. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.6.1.1: Roller og ansvarsområder for Informationssikkerhed - Alle ansvarsområder for Informationssikkerhed er defineret og fordelt på funktionsroller/medarbejdere.	Vi har udført forespørgsler hos passende personale og inspiceret serviceleverandørens politik for Informationssikkerhed. Vi har inspiceret, at roller og ansvarsområder for Informationssikkerhed er klart defineret i serviceleverandørens politik for Informationssikkerhed.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.7 - Medarbejdersikkerhed

Kontrolmål:

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til. DS/ISO IEC 27002:2017*
- *At sikre, at medarbejdere og kontrahenter er bevidste og lever op til deres informationssikkerhedsansvar. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.7.1.1: Screening ▶ Ved ansættelser sker der en vurdering af kandidatens kvalifikationer og der indhentes referencer og straffeattest i nødvendigt omfang.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for ansættelse. Vi har observeret, at der skal indhentes straffeattest og referencer for ansøgere i det omfang, som det vurderes nødvendigt for ansættelsen.	Ingen afvigelser konstateret.
A.7.1.2: Ansættelsesvilkår og betingelser ▶ Ved ansættelser udarbejdes der formelle ansættelseskontrakter/breve som indeholder ansvarsområde, vilkår og betingelser for ansættelsen, herunder tavshedspligt.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for ansættelse. Vi har inspiceret, at proceduren fastsætter retningslinjer for ansættelsesvilkår og betingelser samt ansvarsområder. Vi har inspiceret en stikprøve på en ansættelseskontrakt og observeret, at medarbejdere informeres om ansvar for Informationssikkerhed, herunder tavshedspligt.	Ingen afvigelser konstateret.
A.7.2.2: Bevidsthed om uddannelse og træning i Informationssikkerhed ▶ Ledelsen skal sikre at alle medarbejdere bliver bekendt med informationssikkerhedspolitikken ved ansættelse og at sikkerhedskrav løbende vedligeholdes gennem træning og awareness.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for træning i Informationssikkerhed. Vi har på forespørgsel fået oplyst, at serviceleverandøren årligt afholder MUS-samtaler med alle medarbejdere, blandt andet	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.7 - Medarbejdersikkerhed

Kontrolmål:

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til. DS/ISO IEC 27002:2017*
- *At sikre, at medarbejdere og kontrahenter er bevidste og lever op til deres informationssikkerhedsansvar. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	for at sikre, at medarbejderne har de fornødne kompetencer og uddannelser. Vi har på forespørgsel fået oplyst, at serviceleverandøren årligt gennemgår virksomhedens procedurer og politikker på et fælles møde med alle ansatte. Vi har inspiceret dokumentation for afholdt ISAE møder hver 3. måned og observeret, at det er senest afholdt i april 2023.	
A.7.3.2: Sanktioner - Der er etableret en formel og kommunikeret sanktionsproces, så der skrides ind over for medarbejdere, der begår informationssikkerhedsbrud.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedurer for ansættelse. Vi har inspiceret, at serviceleverandørens skabelon for indgåelse af ansættelseskontrakter indeholder bestemmelser vedrørende sanktionering af medarbejdere ved brud på informationssikkerheden. Vi har inspiceret en stikprøve på en ansættelseskontrakt og observeret, at medarbejdere informeres om sanktioner ved brud på informationssikkerheden. Vi har på forespørgsel fået oplyst, at der ikke findes eksempler på sanktioner i erklæringsperioden.	Ingen afvigelser konstateret.
A.7.3.1: Ansættelsesforholdets ophør eller ændring - Informationssikkerhedsansvar og -forpligtigelser, som gælder efter ansættelsens ophør eller ændring, er defineret og kommunikeret til medarbejdere og kontrahenter og håndhæves.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for ansættelse.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.7 - Medarbejdersikkerhed

Kontrolmål:

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til. DS/ISO IEC 27002:2017*
- *At sikre, at medarbejdere og kontrahenter er bevidste og lever op til deres informationssikkerhedsansvar. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret dokumentation for, at medarbejdere gøres bekendt med deres ansvar efter ansættelsesforholdets ophør.	

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.11 - Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.11.1.1: Fysisk perimetersikring - Krav til fysisk perimetersikring er formelt fastsat. - Ledelsen fører tilsyn med at fysisk perimetersikring forefindes som fastsat i de definerede krav, herunder	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og forsyningssikkerhed. Vi har foretaget fysisk inspektion af serviceleverandørens kontorlokaler og datacentre og observeret, at områderne omkring bygningerne er videoovervåget og at adgang kun kan ske via indgangssluse ved anvendelse af adgangskort med personlig kode. Vi har desuden observeret, at der til datacentre og kontorfaciliteter er installeret AIA-anlæg. Vi har inspiceret forholdsregler for adgang og ophold i datacentre.	Ingen afvigelser konstateret.
A.11.1.2: Fysisk adgangskontrol (eksterne og interne) - Der forefindes en procedure for adgangskontrol til selskabets datacentre som omfatter interne og eksterne personers adgang. - Adgang til datacentre revurderes regelmæssigt, og adgange fjernes hvis der ikke længere er et behov for disse adgange.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og adgangskontrol. Vi har observeret, at adgang til serviceleverandørens datacentre og kontorfaciliteter sker ved anvendelse af adgangskort med personlig kode. Vi har inspiceret udtræk over adgangskort til datacentrene og stikprøvevis inspiceret bestilling af adgangskort og observeret, at udstedelse er sket i henhold til proceduren. Vi har inspiceret adgangslog til datacentre og observeret, at adgang logges i henhold til proceduren.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.11 - Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.11.1.3: Sikring af kontorer, lokaler og faciliteter ▶ Fysisk sikring af kontorer, lokaler og faciliteter er tilrettelagt og etableret.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed. Vi har foretaget fysisk inspektion af serviceleverandørens kontorlokaler og datacentre og observeret, at områderne omkring bygningerne er videoovervåget og at adgang kun kan via indgangssluse ved anvendelse af adgangskort med personlig kode. eller med fysisk nøgle til udvalgte områder. Vi har inspiceret liste med oversigt over udleverede fysiske nøgler samt oversigt over adgangskort til alle datacentre og observeret, at der er opsat logning af adgange til datacenter.	Ingen afvigelser konstateret.
A.11.1.4: Beskyttelse mod eksterne og miljømæssige trusler ▶ Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret, herunder: ○ Vand detektering ○ Brand detektering ○ Indretning af maskinstuer mod opstigende vand/skybrud ○ Indretning mod indbrud/uautoriseret indtrængning.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og årshjul for kontroller. Vi har inspiceret den fysiske sikkerhed for datacentrene i Skanderborg, Randers, Viby J og Aarhus, og observeret, at der i datacentrene er installeret følere for vand og fugt, samt at gulvet er udført i antistatisk materiale og hævet. Vi har observeret, at serviceleverandøren har installeret "sniffer" i datacentre og teknikrum, der analyserer luften for røgpartikler. Vi har observeret, at der er installeret automatisk brandslukning med Inergen i datacentre og teknikrum.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.11 - Fysisk sikring og miljøsikring		
Kontrolmål ▶ *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. DS/ISO IEC 27002:2017*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har observeret, at serviceleverandøren har installeret redundante UPS og dieselgeneratorer, redundant elforsyning og redundant køling i alle datacentre. Vi har observeret, at der er opsat fjernadgang til udstyr samt heartbeat-test til overvågning af alarmfunktionalitet (SMS). Vi har inspiceret log fra alarmsystemer fra datacentrene og observeret, at der er sendt adviseringer i henhold til procedure for området. Vi har inspiceret servicerapporter fra sidste lovpligtige eftersyn, der blev udført i henhold til årshjulet.	
A.11.1.5: Arbejde i sikre områder ▶ Der er etableret procedure for at arbejde i sikre områder og intern såvel om eksterne.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og husregler. Vi har inspiceret informationsfolder til kunder ved udlevering af adgangskort, hvor der informeres om serviceleverandørens husregler og derved krav til sikkerhed i serviceleverandørens datacentre. Vi har observeret, at serviceleverandørens husregler desuden er placeret synligt for kunderne ved indgangen til datacentrene samt rundt i datacentrene. Vi har stikprøvevis observeret, at der ved adgang til datacentre skal kvitteres for, at den enkelte har læst betingelserne for adgang til serviceleverandørens datacenter.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.11 - Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.11.1.6: Områder til af- og pålæsning ▶ Adgangssteder som områder til af- og pålæsning og andre steder, hvor uautoriserede personer kan komme ind på området, er styret og så vidt muligt adskilt fra informationsbehandlings-faciliteter for at minimere risici for uautoriseret adgang.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed. Vi har observeret, at af- og pålæsning ved datacentret i Skanderborg, sker bag ved bygningen. Vi har endvidere observeret, at området er videoovervåget, og at kameraerne overvåges af Jyske kontrolcentral. Vi har observeret, at af- og pålæsning ved datacentret i Aarhus sker foran bygningen på parkeringspladsen ved datacentret. Vi har endvidere observeret, at området er videoovervåget, og at kameraerne overvåges af Jyske kontrolcentral. Vi har observeret, at af- og pålæsning ved datacentret i Randers sker bag bygningen på parkeringspladsen ved datacentret. Vi har endvidere observeret, at området er videoovervåget, og at bygningens udlejer står for overvågningen. Vi har observeret, at af- og pålæsning ved datacentret i Viby J sker bag ved bygningen på parkeringspladsen ved datacentret. Vi har endvidere observeret, at området er videoovervåget, og at kameraerne overvåges af Jyske kontrolcentral. Vi har inspiceret, at serviceleverandørens husregler stiller krav om, at der ikke må tages brandbart materiale med i datacentrene, og at pap og brandbart materiale ikke må efterlades, men skal smides ud i containerne. Vi har observeret, at adgang til datacentret for kunder sker via indgangssluse ved anvendelse af adgangskort med personlig kode.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.11 - Fysisk sikring og miljøsikring

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.11.2.2: Understøttende forsyninger (forsyningssikkerhed) - Krav til forsyningssikring er fastsat og formaliseret. - Der er etableret sikringsforanstaltninger til at imødegå tab af strøm og køling - Anlæg til sikring af forsyningssikkerheden vedligeholdes og afprøves efter fastsatte retningslinjer og i overensstemmelse med leverandørerne anvisninger.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed. Vi har observeret, at serviceleverandøren har standby-generatorer og redundante UPS-anlæg. Vi har inspiceret, at generatorer og UPS-anlæg testes og vedligeholdes regelmæssigt i henhold til serviceleverandørens årshjul og producenternes specifikationer herfor. Vi har inspiceret rapporter for udførte månedlige eftersyn af datacentrene i Skanderborg, Randers, Viby J og Aarhus.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring

Kontrolmål

- *At informationssikkerhedskontinuiteten er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring. DS/ISO IEC 27002:2017*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.17.1.1 Planlægning af informationssikkerhedskontinuitet ▶ Ledelse har fastsat krav til informationssikkerheds-kontinuitet ud fra en risikovurdering.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for risikosty-ring og beredskab samt årshjul for udførelse af kontroller. Vi har inspiceret, at risikovurdering, kapacitetsberegning og be-redskabsplan vurderes hvert år i juni måned. Vi har inspiceret, at der foreligger en ledelsesgodkendt bered-skabsplan, der er tilgængelig for relevante medarbejdere.	Ingen afvigelser konstateret.
A.17.1.2 Implementering af informationssikkerhedskontinui-tet ▶ Der er fastlagt, dokumenteret, implementeret og ved-ligeholdt processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinui-tet i en kritisk situation.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for risikosty-ring og beredskab samt årshjul for udførelse af kontroller. Vi har inspiceret, at beredskabsplan er kendt, samt at ansvars-områder er kendt og formidlet.	Ingen afvigelser konstateret.
A.17.1.3 Verificering, gennemgang og evaluering af informa-tionssikkerhedskontinuiteten ▶ Etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten verificeres med jævne mellemrum med henblik på at sikre, at disse er tidssvarende og effektive i kritiske situationer.	Vi har udført forespørgsler hos passende personale. Vi har inspiceret serviceleverandørens procedure for risikosty-ring og beredskab samt årshjul for udførelse af kontroller. Vi har inspiceret, at risikovurdering og beredskabsplan skal vur-deres hvert år i juni måned.	Ingen afvigelser konstateret.

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

A.17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring		
Kontrolmål ▶ *At informationssikkerhedskontinuiteten er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring. DS/ISO IEC 27002:2017*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har inspiceret, at risikovurdering senest er opdateret den d. 14. april 2023, og at beredskabsplanen senest er vurderet den d. 14. april 2023. Vi har inspiceret dokumentation for udført beredskabstest og observeret, at den blev udført d. 16. februar 2023.	

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 80

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 medlemsfirmaer. BDO er varemærke for både BDO-netværket og for alle BDO medlemsfirmaerne. BDO i Danmark beskæftiger mere end 1.400 medarbejdere, mens det verdensomspændende BDO-netværk har ca. 111.000 medarbejdere i mere end 167 lande.

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

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

PENNEO

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

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

Mikkel Jon Larssen
BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670
Partner
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2023-07-10 09:45:49 UTC
MitID

Christian Holm Christensen
Direktør
Serienummer: 6778a938-9621-4a65-92d3-6294281b8d81
IP: 80.208.xxx.xxx
2023-07-11 10:24:43 UTC
MitID

Nicolai Tobias Visti Pedersen
Statsautoriseret revisor
Serienummer: CVR:20222670-RID:1283706411033
IP: 77.243.xxx.xxx
2023-07-11 11:10:24 UTC
NEM ID

Penneo dokumentnøgle: 6QD0K-1PC8N-0EJI1-TTTGD-82I4E-Y3MSJ

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske s igneringsbeviser i ndlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**