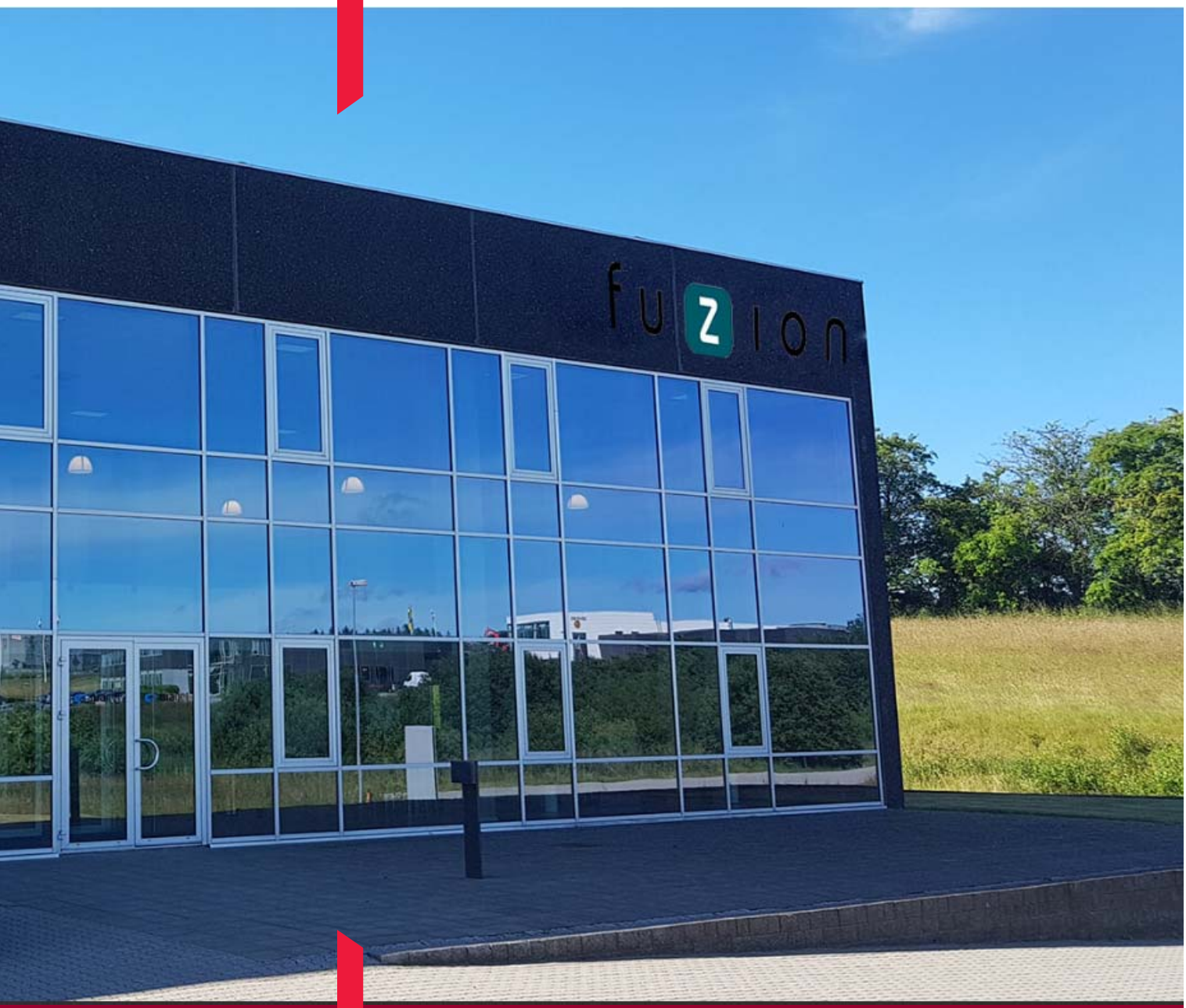



# ISAE 3402-ERKLÆRING PR. 1. JULI 2019 OM BESKRIVELSEN AF DATACENTER-LØSNING OG DE FYSISKE SIKKERHEDSFORANSTALTNINGER (KONTROLLER) OG DERES UDFORMNING

FUZION A/S

BDO

# INDHOLD

# REVISORS ERKLÆRING

## UAFHÆNGIG REVISORS ERKLÆRING MED SIKKERHED OM BESKRIVELSEN AF DATACENTER-LØSNING OG DE FYSISKE SIKKERHEDSFORANSTALTNINGER (KONTROLLER) OG DERES UDFORMNING

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

### Omfang

Vi har fået som opgave at afgive erklæring om den af Fuzion A/S (serviceleverandøren) udarbejdede beskrivelse på side 5 - 8 om Datacenter-løsning og de fysiske sikkerhedsforanstaltninger (kontroller), og om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

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

### Serviceleverandørens ansvar

På side 4 i nærværende rapport har serviceleverandøren afgivet en udtalelse om egnetheden af den samlede præsentation af beskrivelsen samt hensigtsmæssigheden af de udformede kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandøren er ansvarlig for udarbejdelsen af beskrivelsen og udtalelsen, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret. Serviceleverandøren er endvidere ansvarlig for leveringen af de ydelser, beskrivelsen omfatter, ligesom serviceleverandøren er ansvarlig for at anføre kontrolmålene og identificere de risici, som truer opnåelsen af kontrolmålene, samt udforme og implementere effektivt fungerende kontroller for at nå de anførte kontrolmål.

### Revisors uafhængighed og kvalitetsstyring

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

Vi anvender ISQC 1 og opretholder derfor et omfattende system for kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav ifølge lov og øvrig regulering.

### Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om serviceleverandørens beskrivelse samt om udformningen af de kontroller, der knytter sig til de kontrolmål, som er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af International Auditing and Assurance Standards Board. Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå høj grad af sikkerhed for, om beskrivelsen i alle væsentlige henseender er retvisende, og om kontrollerne i alle væsentlige henseender er hensigtsmæssigt udformet.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen og udformningen af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse samt for kontrollernes udformning. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at beskrivelsen ikke er retvisende, og at kontrollerne ikke er hensigtsmæssigt udformet. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet på side 4.

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

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

**Begrænsninger i kontroller hos en serviceleverandør**

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

**Konklusion**

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, vi har anvendt ved udformningen af konklusionen, er de kriterier, der er beskrevet i serviceleverandørens udtalelse på side 4. Det er vores opfattelse:

a. at beskrivelsen Datacenter-løsning og de fysiske sikkerhedsforanstaltninger (kontroller), således som disse var udformet og implementeret pr. 1. juli 2019, i alle væsentlige henseender er retvisende, og

b. at de fysiske sikkerhedsforanstaltninger (kontrollerne), som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet pr. 1. juli 2019.

**Beskrivelse af test af kontroller**

De specifikke kontroller, der er blevet testet, og resultater af disse test fremgår på side 10 - 19.

**Tiltænkte brugere og formål**

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

København, den 5. juli 2019

**BDO Statsautoriseret revisionsaktieselskab**

Per Sloth
Partner, chef for Risk Assurance
Registreret revisor

Mikkel Jon Larssen
Partner, CISA, CRISC

# FUZION A/S' UDTALELSE

Fuzion A/S har udarbejdet medfølgende beskrivelse af Datacenter-løsning og de fysiske sikkerhedsforanstaltninger (kontroller).

Beskrivelsen er udarbejdet til brug for Fuzion A/S' 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 kundernes informationssystemer, som er relevante for regnskabsaflæggelsen.

Fuzion A/S bekræfter, at den medfølgende beskrivelse på side 5 – 8 giver en retvisende beskrivelse af Datacenter-løsning og de fysiske sikkerhedsforanstaltninger (kontroller) pr. 1. juli 2019. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for, hvordan de fysiske sikkerhedsforanstaltninger i tilknytning til Datacenter-løsning var udformet og implementeret, herunder redegør for:
    - De typer af ydelser, der er leveret.
    - De processer i både informationsteknologiske og manuelle systemer, der er anvendt til styring af de fysiske sikkerhedsforanstaltninger (kontroller).
    - De relevante kontrolmål og kontrolaktiviteter, der er udformet for at nå disse mål.
    - Andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne, kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for kundernes Datacenter-løsning.
2. Den medfølgende beskrivelse ikke udelader eller forvansker information, der er relevant for omfanget af beskrivelsen af Datacenter-løsning og de fysiske sikkerhedsforanstaltninger (kontroller) under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer, og derfor ikke kan omfatte ethvert aspekt ved Datacenter-løsningen, som den enkelte kunde måtte anse for vigtigt efter deres særlige forhold.

Fuzion A/S bekræfter, at de fysiske sikkerhedsforanstaltninger (kontroller), der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet pr. 1. juli 2019. Kriterierne for denne udtalelse var, at:

1. De risici, som truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.
2. De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål.

Skanderborg, den 5. juli 2019

Fuzion A/S
Adm. Direktør Per Henriksen

# FUZION A/S' BESKRIVELSE

## BESKRIVELSE AF KONTROLMILJØET I FORBINDELSE MED FUZION A/S' CO-LOCATION SERVICES

### Indledning

Formålet med nærværende beskrivelse er at levere information til Fuzion A/S' (Fuzion) kunder og deres revisorer med henblik på få afgivet en ISAE 3402-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.

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

Beskrivelsen er udarbejdet for at opfylde de typiske behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan 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.

### 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 har gennem flere år været en førende udbyder af datacentre i det vestlige Danmark.

I 2010 blev Fuzion købt af Nianet, som i forvejen havde en omfattende fiber og datacenterforretning, og Fuzion skiftede navn til Nianet. I 2017 blev Nianet købt af GlobalConnect og i den forbindelse blev det aftalt med Forbruger- og Konkurrencestyrelsen, at de oprindelige Fuzion-datacentre skulle sælges for at sikre fortsat konkurrence på datacenter/co-location markedet i Jylland. Derfor har Fuzion siden 2018 været ejet af en dansk investor og iværksætter med erfaring fra infrastruktur, kundeservice og online tjenester.

Fuzion leverer datacenterinfrastruktur til kunder med forretningskritiske it-systemer og er en førende co-location leverandør med sikre og energieffektive datacentre i Skanderborg og Aarhus. 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 til for eksempel at levere cloud, hosting, online applikationer og internetløsninger.

### Fuzions co-location services

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

Fuzions datacentre er designet og bygget efter anerkendte, internationale standarder for sikre datacentre og er løbende moderniseret, udvidet og effektiviseret med nogle af 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 stort antal kunder med stor fleksibilitet og sikker adskillelse af kundernes infrastruktur. Flere af kunderne bruger begge Fuzions to datacentre, da brugen af de to datacentre giver meget høj redundans og samtidigt tilbyder sig med en fornuftig køreafstand mellem de to centre.

### 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 for private og public Cloud, IOT, online apps, internet og meget mere – nu og i fremtiden.

Fuzion har en klar strategi om at opnå vækst ved at levere den ønskede kvalitet til markedet til en fornuftig pris og med en god service og meget høj integritet i forhold til kvalitet i test, drift, vedligehold, dokumentation og kommunikation med kunderne.

Fuzions forretning er at levere den nødvendige fysiske sikkerhed og oppetid for den infrastruktur, som Fuzions kunder installerer og drifter i racks, 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.

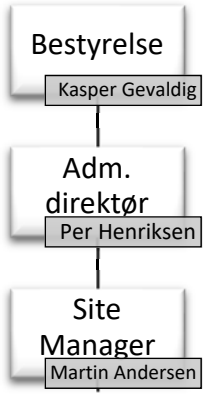
Fuzion skal sikre kundernes infrastruktur med et effektivt værn mod sikkerhedsmæssige trusler. Beskyttelsen er vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Såvel ansatte, gæster, kunder som eksterne personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen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

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

### Fuzions Organisering

Den overordnede ansvarlige for forretningen og sikkerheden er den administrerende direktør (CEO), 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.




### 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.

Fuzion 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.

### Sikkerhedsforanstaltninger adgang og overvågning

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

### 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, medarbejdere, gæster og håndværkere, og beskriver de tiltag og tilladelser, der kræves for at opnå og overvåge adgang.

Al adgang foregår 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.

### Administration af 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 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. Fuzions down-flow får koldt kølevand fra udendørs enheder, der køler vandet med en kombination af frikøl og kompressorkøl. I alle områder kontrolleres og styres temperaturen.

### Brandsikring og slukning

Datacentrene er opført i brandhæmmende materiale og beskyttet af automatiske brandslukningsanlæg, der er koblet til optiske og ioniserende 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 og udløse brandslukning, når det behøves. Dette system kendes også som et VESDA system – Very Early Smoke Detecting Apparatus.

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

### Medarbejdere

Fuzions har etableret en intern proces for ansættelse, der sikrer, at medarbejdere screenes på passende vis, at kontrakten inkluderer en tavshedsklausul, samt at medarbejdere holdes ajour med de relevante sikkerhedskrav og pligter.

### Beredskab

Fuzion har etableret en beredskabsplan, der 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.

# KONTROLMÅL, KONTROLLER, TEST OG RESULTAT AF TEST

I nærværende testskema er relevante kontrolmål og indførte kontrolaktiviteter udformet til at nå kontrolmålene, beskrevet og udvalgt af Fuzion A/S.

I testskemaet har vi beskrevet de udførte test, som blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og de tilhørende kontroller er hensigtsmæssigt udformet pr. 1. juli 2019.

Test af kontrollernes design og implementering er udført ved forespørgsel, inspektion og observation.

| Type | Beskrivelse |
|---|---|
| **Forespørgsel** | Forespørgsler hos passende personale hos Fuzion A/S 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. |

| A.5 - Informationssikkerhedspolitikker | | |
|---|---|---|
| **Kontrolmål**<br>• *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 informationssikkerhed**<br>Med udgangspunkt i en risikovurdering fastlægger og godkender ledelsen et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter. | Vi har observeret, at der foreligger en ledelsesgodkendt it-sikkerhedspolitik.<br><br>Vi har observeret, at ledelsen sikrer, at medarbejderne bliver gjort bekendt med it-sikkerhedspolitikken.<br><br>Vi har observeret, at serviceleverandørens risikovurdering er godkendt af ledelsen den 7. juni 2019 | Ingen afvigelser konstateret |
| **A.5.1.2: Gennemgang af politikkerne for informationssikkerhed**<br>Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet. | Vi har udført forespørgsler hos passende personale og inspiceret serviceleverandørens politik for informationssikkerhed<br><br>Vi har observeret, at serviceleverandørens informationssikkerhedspolitik er godkendt af ledelsen den 7. juni 2019. Vi har inspiceret årshjul og observeret, at informationssikkerhedspolitikken skal gennemgås en gang årligt.<br><br>Vi har endvidere observeret, at ledelsen erklærer, at medarbejdere har læst og forstået relevante sikkerhedskrav. | Ingen afvigelser konstateret |

| A.6 - Organisering af informationssikkerhed | | |
|---|---|---|
| **Kontrolmål**<br>• *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**<br>Alle ansvarsområder for informationssikkerhed er defineret og fordelt. | Vi har udført forespørgsler hos passende personale og inspiceret serviceleverandørens politik for informationssikkerhed<br><br>Vi har observeret, at roller og ansvarsområder for informations-sikkerhed er klart defineret i serviceleverandørens politik for informationssikkerhed. | Ingen afvigelser konstateret |

## 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**<br>Efterprøvning af alle jobkandidaters baggrund er udført i overensstemmelse med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikation af den information, der gives adgang til, og de relevante risici. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for ansættelse.<br><br>Vi har observeret, at der skal indhentes straffeattest og referencer for ansøgere i det omfang, som det vurderes nødvendigt for ansættelsen.<br><br>Vi har ikke kunnet efterprøve procedure for ansættelse, idet der ikke har været ansat nye medarbejdere på tidspunktet for erklæringsafgivelsen. | Ingen afvigelser konstateret |
| **A.7.1.2: Ansættelsesvilkår og betingelser**<br>Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for Informationssikkerhed. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for ansættelse.<br><br>Vi har observeret, at proceduren fastsætter retningslinjer for ansættelsesvilkår og betingelser samt ansvarsområder.<br><br>Vi har inspiceret en stikprøve på en ansættelseskontrakt og observeret, at medarbejdere informeres om ansvar for informationssikkerhed, herunder tavshedspligt. | Ingen afvigelser konstateret |
| **A.7.1.3: Bevidsthed om uddannelse og træning i informationssikkerhed**<br>Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter bliver ved hjælp af uddannelse og træning bevidstgjort om sikkerhed og bliver regelmæssigt holdt ajour om organisationens politikker og procedurer, i det omfang dette er relevant for deres jobfunktion. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for træning i informationssikkerhed.<br><br>Vi har observeret, at medarbejdere bliver informeret om krav til uddannelse og kompetenceløft. | Ingen afvigelser konstateret |

## 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 ikke kunnet efterprøve procedure for bevidsthed om uddannelse, idet der ved tidspunkt for erklæringsafgivelse ikke var ansat personale med mere en 6 måneders anciennitet. | |
| **A.7.1.4: Sanktioner**<br>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.<br><br>Vi har inspiceret serviceleverandørens procedurer for ansættelse.<br><br>Vi har observeret, at serviceleverandørens skabelon for indgåelse af ansættelseskontrakter indeholder bestemmelser vedrørende sanktionering af med arbejdere ved brud på informationssikkerheden.<br><br>Vi har inspiceret en stikprøve på en ansættelseskontrakt og observeret, at medarbejdere informeres om sanktioner ved brud på informationssikkerheden. | Ingen afvigelser konstateret |
| **A.7.1.5: Ansættelsesforholdets ophør eller ændring**<br>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.<br><br>Vi har inspiceret serviceleverandørens procedure for ansættelse.<br><br>Vi har observeret, at procedure for ansættelser angiver at medarbejdere gøres bekendt med deres ansvar efter ansættelsesforholdets ophør.<br><br>Vi har fået oplyst, at der på tidspunktet for erklæringsafgivelsen ikke har været fratrædelse af medarbejdere hvorfor vi ikke har kunne teste om kontrollen er implementeret. | Ingen afvigelser konstateret |

## 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**<br>Der er defineret og anvendt perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed.<br><br>Vi har foretaget fysisk inspektion af serviceleverandørens fysiske kontorlokaler og datacentre og observeret, at området omkring bygningerne er videoovervåget og adgang kun kan ske med personligt adgangskort med kode.<br><br>Vi har endvidere observeret, at der til datacentre og kontorfaciliteter er installeret AIA-anlæg.<br><br>Vi har observeret, at der i datacentrene er installeret vand- og fugt følere, samt at gulvet er udført i antistatisk materiale og hævet.<br><br>Vi har observeret, at der er opsat retningslinjer for fysisk perimetersikring af anlæg i Skanderborg og Aarhus. | Ingen afvigelser konstateret |
| **A.11.1.2: Fysisk adgangskontrol (eksterne og interne)**<br>Sikre områder er beskyttet med passende adgangs- kontrol for at sikre, at kun autoriseret personale kan få adgang. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og fysisk adgangskontrol.<br><br>Vi har observeret, at adgang til serviceleverandørens datacentre og kontorfaciliteter sker med adgangskort med personlig kode.<br><br>Vi har udtaget en stikprøve på bestilling af adgangskort og observeret, at dette er udstedt i henhold til proceduren herfor.<br><br>Vi har inspiceret adgangslog til datacentre og observeret, at adgang logges i henhold til procedure på området. | Ingen afvigelser konstateret |

## 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**<br>Fysisk sikring af kontorer, lokaler og faciliteter er tilrettelagt og etableret. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed.<br><br>Vi har foretaget fysisk inspektion af serviceleverandørens kontorlokaler og datacentre og observeret, at området omkring bygningerne er videoovervåget, og at adgang kun kan ske med personligt adgangskort med kode, eller med fysisk nøgle til udvalgte områder.<br><br>Vi har observeret, at der er udarbejdet en liste med oversigt over udleverede fysiske nøgler samt oversigt over adgangskort til begge datacentre. Vi har inspiceret, at der er foretaget logning af adgange til datacenter. | Ingen afvigelser konstateret |
| **A.11.1.4: Beskyttelse mod eksterne og miljømæssige trusler**<br>Fysisk beskyttelse mod naturkatastrofer, ondsindede angreb eller ulykker er tilrettelagt og etableret. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og årshjul.<br><br>Vi har inspiceret den fysiske sikkerhed for datacenter i Skanderborg og Aarhus.<br><br>Vi har observeret, at serviceleverandøren har installeret redundant UPS og dieselgeneratorer, redundant elforsyning, redundant køling til alle rum samt brandslukning med røgalarmer i teknik og serverrum.<br><br>Vi har observeret, at der er opsat fjernadgang til overvågning af udstyr samt heartbeat test til overvågning af alarm funktionalitet (SMS).<br><br>Vi har inspiceret log fra alarmsystem ved datacenter og observeret, at der er sendt advisering i henhold til procedure på området. | Vi konstaterer, at der i datacentret i Aarhus ikke er foretaget udskiftning af en Inergen-flaske ved brandslukningsanlægget i henhold til leverandørens anvisninger herfor.<br><br>Ingen øvrige afvigelser konstateret. |

| A.11 - Fysisk sikring og miljøsikring | | |
|---|---|---|
| **Kontrolmål**<br>• *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 inspiceret servicerapport fra sidste lovpligtige eftersyn, der blev udført i 2018. | |
| **A.11.1.5: Arbejde i sikre områder**<br>Der er etableret procedure for at arbejde i sikre områder. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed og husregler.<br><br>Vi har fået oplyst, at kunder ved udlevering af adgangskort informeres om serviceleverandørens husregler og derved krav til sikkerhed i serviceleverandørens datacentre.<br><br>Vi har observeret, at serviceleverandørens husregler er placeret synligt for kunderne ved indgangen til datacentrene i Skanderborg og Aarhus samt rundt i datacentrene.<br><br>Vi har stikprøvevis observeret, at der ved adgang til datacenter skal kvitteres for at have læst betingelser for adgang til serverrum hos serviceleverandøren. | Ingen afvigelser konstateret |
| **A.11.1.6: Områder til af- og pålæsning**<br>Adgangssteder som fx 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 undgå uautoriseret adgang. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed.<br><br>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.<br><br>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. | Ingen afvigelser konstateret |

| A.11 - Fysisk sikring og miljøsikring | | |
|---|---|---|
| **Kontrolmål**<br>• *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 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.<br><br>Vi har observeret, at adgang til datacentret for kunder sker via indgangssluse med adgangskort med personlig kode. | |
| **A.11.1.7: Understøttende forsyninger (forsyningssikkerhed)**<br>Udstyr er beskyttet mod strømsvigt og andre forstyrrelser som følge af svigt af understøttede forsyninger. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for fysisk sikkerhed.<br><br>Vi har observeret, at serviceleverandøren har standby-generatorer og redundant UPS-anlæg.<br><br>Vi har ved stikprøver observeret, at generatorerne og UPS testes og vedligeholdes regelmæssigt i henhold til serviceleverandørens årshjul og producenternes specifikationer.<br><br>Vi har inspiceret rapport for udført månedligt eftersyn af datacenter i Skanderborg og Aarhus. | Ingen afvigelser konstateret |

| A.17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring | | |
|---|---|---|
| **Kontrolmål**<br>• *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**<br>Der er fastlagt en ensartet ramme for virksomhedens beredskabsplaner for at sikre, at alle planerne er sammenhængende og tilgodeser alle sikkerhedskrav, samt for at fastlægge prioriteringen af afprøvning og vedligeholdelse. Kontrol af Informationssikkerhedskontinuiteten er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for risikostyring og beredskab samt årshjul for udførelse af kontroller.<br><br>Vi har observeret, at risikovurdering, kapacitetsberegning og beredskabsplan skal vurderes hvert år i juni måned.<br><br>Vi har observeret, at der foreligger en ledelsesgodkendt beredskabsplan, der er tilgængelig for relevante medarbejdere. | Ingen afvigelser konstateret |
| **A.17.1.2 Implementering af informationssikkerhedskontinuitet**<br>Der er fastlagt, dokumenteret, implementeret og vedligeholdt processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for risikostyring og beredskab samt årshjul for udførelse af kontroller.<br><br>Vi har observeret, at risikovurdering, kapacitetsberegning og beredskabsplan skal vurderes hvert år i juni måned<br><br>Vi har observeret, at beredskabsplan er kendt, samt at ansvar områder er kendt og formidlet.<br><br>Vi har inspiceret serviceleverandørens årshjul og observeret, at test af beredskab skal finde sted i oktober måned. Det har derfor ikke været muligt at indhente dokumentation for udførelse af beredskabstest. | Ingen afvigelser konstateret |

| A.17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring | | |
|---|---|---|
| **Kontrolmål**<br>• *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.17.1.3 Verificering, gennemgang og evaluering af informations-sikkerhedskontinuiteten**<br>Etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten verificeres med jævne mellemrum med henblik på at sikre at der er tidssvarende og effektive i kritiske situationer. | Vi har udført forespørgsler hos passende personale.<br><br>Vi har inspiceret serviceleverandørens procedure for risikostyring og beredskab samt årshjul for udførelse af kontroller.<br><br>Vi har observeret at risikovurdering, kapacitetsberegning og beredskabsplan skal vurderes hvert år i juni måned.<br><br>Vi har inspiceret serviceleverandørens årshjul og observeret, at test af beredskab skal finde sted i oktober måned. Det har derfor ikke været muligt at indhente dokumentation for udførelse af beredskabstest. | Ingen afvigelser konstateret |

**BDO Statsautoriseret revisionsaktieselskab**

**Havneholmen 29**
**DK-1561 København V**
**CVR-nr. 20 22 26 70**

*BDO Statsautoriseret revisionsaktieselskab, en 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 godt 1.200 medarbejdere, mens det verdensomspændende BDO netværk har godt 80.000 medarbejdere i 162 lande.*

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