NEM IT-SOLUTIONS A/S

AFGIVELSE AF UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2021 OM BESKRIVELSEN AF HOSTINGPLATFORMEN OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

BDO

INDHOLD

1. UAFHÆNGIG REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ISAE 3402-ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2021 OM BESKRIVELSEN AF HOSTINGPLATFORMEN OG DE TILHØRENDE KONTROLLER, DERES UDFORMNING OG OPERATIONELLE EFFEKTIVITET

Til: Ledelsen i NEM It-solutions A/S
NEM It-Solutions kunder og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om den af NEM It-solutions (serviceleverandøren) for hele perioden 1. januar til 31 december 2021 udarbejdede beskrivelse i sektion 3 af Hostingplatformen og de tilhørende kontroller, 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.

Vi er underlagt den internationale standard om kvalitetsstyring ISQC 1, og vi anvender og opretholder således et omfattende kvalitetsstyringssystem, 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 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

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 Hostingplatformen, 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 Hostingplatformen og de tilhørende kontroller, således som de var udformet og implementeret i hele perioden fra 1. januar til 31. december 2021, 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. januar til 31. december 2021, 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. januar til 31. december 2021.

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 Hostingplatformen, 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 21. juni 2022

BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. NEM IT-SOLUTIONS UDTALELSE

NEM It-solutions A/S løser opgaver inden for It-drift og support.

Medfølgende beskrivelse er udarbejdet til brug for kunder, der anvender NEM It-solutions A/S' hostingydelser, og deres revisorer, som har en tilstrækkelige 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.

NEM It-solutions A/S anvender serviceunderleverandør. Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse.

NEM It-solutions A/S bekræfter, at den medfølgende beskrivelse i sektion 3 giver en retvisende beskrivelse af Hostingplatformen og de tilhørende kontroller i hele perioden fra 1. januar til 31. december 2021. Kriterierne anvendt for at give denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for Hostingplatformen, og, hvordan de tilhørende kontroller var udformet og implementeret, herunder redegør for:
    - De typer af ydelser, der er leveret i forbindelse med driften af Hostingplatformen.
    - De processer og kontroller der indgår i driften af Hostingplatformen.
    - 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.
    - Relevante kontrolmål og kontroller udformet til at nå disse mål.
    - Kontroller, som vi med henvisning til Hostingplatformens udformning har forudsat ville være implementeret af kunder, 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 Hostingplatformen foretaget i perioden fra 1. januar til 31. december 2021.
3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af Hostingplatformen 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 Hostingplatformen, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

NEM It-solutions 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. januar til 31. december 2021. 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. januar til 31. december 2021.

Herlev, den 21. juni 2022

NEM It-solutions

Hans-Henrik Skaarup
Adm. direktør

3. NEM IT-SOLUTIONS BESKRIVELSE AF HOSTINGPLATFORMEN

INTRODUKTION

Formålet med denne beskrivelse er, at levere information til NEM It-solutions A/S kunder, og deres revisorer, vedrørende kravene i den internationale revisionsstandard for erklæringsopgaver om kontroller hos en serviceleverandør, ISAE 3402.

Beskrivelsen har herudover det formål, at give information om de kontroller, der er anvendt for vores hostingsystem fra ultimo august 2019.

Følgende beskrivelse omfatter de kontrolmål og kontroller hos NEM It-solutions A/S, som omfatter størstedelen af vores kunder og er baseret på vores standardleverance. Individuelle kundeforhold, er ikke medtaget i denne beskrivelse.

OM NEM IT-SOLUTIONS A/S

NEM It-solutions A/S er en 100 % danskejet virksomhed, der siden 2003 har specialiseret sig i effektive IT-løsninger for alle typer kunder, små som store.

I NEM It-solutions A/S (i daglig tale kaldet NEM) lægger vi stor vægt på at levere totale løsninger og sørge for samspillet mellem alle de funktioner som IT, telefoni, alarm etc., kræver i dag. Dette betyder, at vi ofte går i dialog med andre leverandører på kundens vegne. Derved undgås de problemer som kan opstå i samspillet mellem flere systemer og leverandører. Vi sætter en ære i at løse en opgave tilfredsstillende uanset art eller størrelse.

NEM ejer i dag et komplet server hosting miljø som supporterer kunder med afdelinger spredt over hele verden. Dette er opstillet i et professionelt og sikkert datacenter med alt hvad dertil hører af overvågning, strømbackup og brandslukning. Systemet er opbygget på en sådan måde, at det hurtigt og nemt kan udbygges.

Vores hosting miljø består blandt andet af terminal servere, hosted Exchange servere, web-servere, SQL servere, backup-servere, overvågning mm. Dette betyder at vi i dag udbyder en bred vifte af services til vores kunder. Populært sagt kan kunden selv vælge hvilke produkter der ønskes, alt efter om kunden ønsker en total hosting løsning eller kun hosting af visse dele. Vi supporterer også lokale servere hos vores kunder.

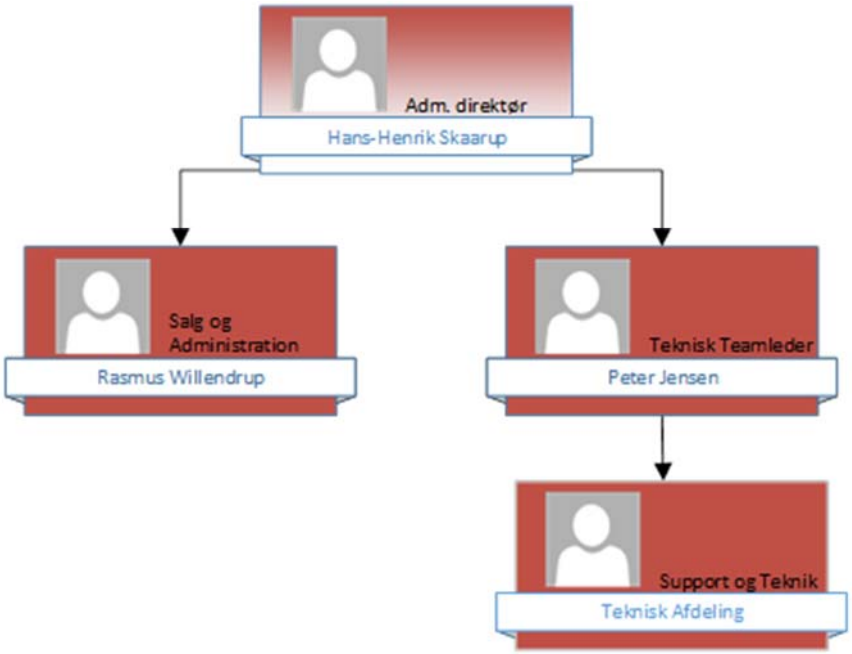
I NEM har vi gennem vores erfarne medarbejdere en meget bred viden inden for IT. Vi kommer fra forskellige IT- og teknik erhverv, hvor arbejdet har været præget af problemløsning og styring af projekter, og vi er derfor godt rustet til at rådgive kunderne omkring totale løsning fra A til Z.

Vi lægger stor vægt på at være fleksible og på at yde vores kunder en smilende og kompetent service. Det er derfor også vigtigt for os at vores kunder til stadighed udtrykker en tilfredshed med vores arbejdsindsats.

ORGANISATION OG ANSVAR

NEM It-solutions A/S er inddelt i afdelingerne Ledelse & administration samt IT & drift. Alle support opgaver varetages hovedsagelig af IT og drift, som modtager alle indkomne forespørgsler. IT og drift har også ansvaret for drift, vedligeholdelse og videreudvikling af vores hostingmiljø.

Ledelsen hos NEM It-solutions A/S har det overordnede ansvar for IT-sikkerheden i virksomheden.



RISIKOSTYRING I NEM IT-SOLUTIONS A/S

Vi har procedurer for løbende risikovurdering af vores forretning. Dermed kan vi sikre, at de risici, som er forbundet med de services og ydelser, vi stiller til rådighed, er minimeret til et acceptabelt niveau.

Vores værktøj til risikostyring er baseret på ISO 27005:2014 (regelsæt for risikoledelse) og risikovurdering foretages løbende samt når vi foretager ændringer eller implementerer nye systemer, som vi vurderer relevante til at revurdere vores generelle risikovurdering.

Ansvaret for risikovurderinger er placeret hos den Tekniske teamleader, og skal efterfølgende forankres og godkendes hos NEM It-solutions A/S ledelse.

GENERELT OM VORES KONTROLMÅL OG IMPLEMENTEREDE KONTROLLER

Vores overordnede kontrolmål er at sikre at de politikker, som vi har angivet i vores samlede informationssikkerhedspolitik, efterleves.

Vores metodik til implementering af kontroller er defineret ud fra ISO 27002:2013 regelsættet for styring af informationssikkerhed og er helt overordnet inddelt i følgende kontrolområder:

4 - Risikovurdering og -håndtering
5 - Informationssikkerhedspolitikker
6 - Organisering af informationssikkerhed
7 - Medarbejdersikkerhed
8 - Styring af aktiver
9 - Adgangsstyring
11 - Fysisk sikring og miljøsikring
12 - Driftssikkerhed
13 - Kommunikationssikkerhed
15 - Leverandørforhold
16 - Styring af informationssikkerhedsbrud

17 - Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
18 - Overensstemmelse

Vi foretager løbende forbedringer af både politikker, procedurer og den operationelle drift. Vi foretager årlig revidering for hvorvidt vi lever op til vores regelsæt der centrerer sig om hvordan vi leverer vores driftsydelser, foretager genetablering, håndterer sikkerhedsopdatering mv.

NEM It-solutions A/S benytter sig af underleverandører i form af levering af de fysiske rammer i forbindelse med datacenteret. Leverancerne drejer sig om levering af fysisk lokation (bygninger), fysisk kontrol, internetforbindelser, adgangssikkerhed samt levering af strøm. Der stilles krav om at disse underleverandører besidder en gyldig ISAE 3402 revisorerklæring.

KONTROLMILJØ

Det følgende beskriver vores kontrolmiljø nærmere for hvert enkelt område.

OVERORDNEDE RETNINGSLINJER

Vi har defineret vores overordnede metodik og tilgang til levering af vores ydelser med hvad dette indebærer, i vores IT-sikkerhedspolitik og tilhørende strategiske og taktiske dokumenter. Formålet er at sikre, at vi har ledelsesgodkendte retningslinjer for informationssikkerhed i forhold til forretningsstrategien - og i forhold til relevant lovgivning. Ledelsens budskab er kommunikeret til alle medarbejdere i NEM It-solutions A/S, og vi opdaterer løbende dokumenterne efter behov, og minimum en gang årligt.

Dette punkt er yderligere beskrevet tidligere i denne beskrivelse, under overskriften 'Generelt om vores kontrolmål og implementerede kontroller'.

ORGANISERING AF INFORMATIONSSIKKERHED

Formål
Styring af sikkerhed, drift, og generel styring af vores processer der munder ud i vores leverance, skal ske ensartet og pålideligt.

Ledelsesopbakning
Det er ledelsen der godkender retningslinjerne for politikker og procedurer, og det er ledelsen der periodisk godkender opdateringer hertil. Årligt foretages der review heraf for at sikre en opdateret politik.

Politik
Vi har etableret en IT-sikkerhedspolitik der beskriver hvordan vi overordnet skal håndtere vores forretning og vores leverance. Alle medarbejdere kender til denne og informeres, når ledelsen godkender opdateringer til politikken.

Vi har en klart opdelt organisation i forhold til informationssikkerhed, og har udførlige ansvars- og rollebeskrivelser for de enkelte medarbejdere.

Der er etableret fortrolighed generelt for alle involverede i vores forretning. Dette sker via ansættelseskontrakter eller samarbejdsaftaler med underleverandører og samarbejdspartnere.

Vi har i vores politik defineret hvordan vi samarbejder med eksterne parter. Er der tale om parter som er en integreret del af vores leverancer, skal vi føre tilsyn med underleverandørens etablerede kontroller.

Vi har etableret en politik og procedure for kontakt til relevante myndigheder i tilfælde af sikkerhedsbrud.

Vores tekniske og logiske sikkerhedsmodel kan ikke afviges. Ønsker kunder ændringer, der efter vores opfattelse slækker på deres eller på vores, eller andre kunders systemer, tager vi en dialog med kunden om en tilsvarende løsning. Dette kan være web-services, kodeordspolitik, IP-forhold mv.

Vi har etableret en intern IT-sikkerhedsorganisation, som sikrer at politikker og procedurer ajourføres og bidrager til optimering af det aktuelle sikkerhedsniveau i NEM It-solutions A/S. IT-sikkerhedsorganisationen afholder faste møder hvert kvartal og ellers efter behov.

STYRING AF INFORMATIONSRELATEREDE AKTIVER

Formål

Systemer, data og enheder, herunder medarbejdere, mm. skal sikres og dokumenteres betryggende.

Ejerskab

Via ansvarsfordeling og rollebeskrivelser, er centrale netværksenheder, servere, periferienheder, systemer og data tilegnet systemansvarlige i vores virksomhed. Kunders data og systemer er tilegnet kundens kontaktperson. Vi arbejder med ejerskab for at sikre, at ingen enheder, systemer eller data bliver glemt ift. sikkerhedsopdatering, klassifikation, drift og vedligehold.

Brug af aktiver

Vi har klart defineret politikker for accepteret brug af aktiver. De gælder både for medarbejdere, såvel som for leverandører. Politikkerne gennemgås og opdateres årligt.

Klassifikation af informationer

Der er lavet en politik for klassifikation af informationer. Vi anser som udgangspunkt alle kundedata som fortrolige. Dette betyder at kun betroede medarbejdere, som har underskrevet en tavshedserklæring, har adgang til systemer og services med kundedata. Udstyr og services, som indeholder kundedata er dokumenteret i vores dokumentationssystem.

Håndtering af aktiver

Som en del af vores IT-sikkerhedspolitik har vi angivet regler for håndtering af aktiver. Medarbejderne er derfor bekendt med hvordan informationer og aktiver klassificeres og hvordan disse skal behandles.

Transport af fysiske medier

I forbindelse med transport af fysiske medier har vi defineret en politik, som har til formå at sikre at medier som indeholder data klassificeret som fortroligt eller til internt brug kun sende med en godkendt transportør.

KONTRAKTER, SLA

Vi tilbyder kontrakter på hostingydelser for vores kunder. Særlige forhold er beskrevet heri, som de var ved aftaleindgåelse.

Vores SLA (Service Level Agreement) beskriver vores generelle vilkår, i forbindelse med vores ydelse overfor vores kunder, responstid, support mv.

FYSISKE ENHEDER

Servere og netværksudstyr inkl. konfiguration er registreret til brug ved dokumentation, overblik over udstyr mv.

MEDARBEJDERE OG DERES CERTIFICERINGER

Vores aktiver er i høj grad vores medarbejdere, og vi fører en struktureret metodik i forhold til vores medarbejderes kvalifikationer, uddannelse og certificeringer.

MEDARBEJDERSIKKERHED

Formål

Vi vil sikre, at alle i virksomheden er bekendte med deres roller og ansvar - herunder også vores underleverandører og 3. parter, og at alle er kvalificerede og egnede til at udføre deres rolle.

Roller og ansvar og samarbejde med eksterne
Alle i vores virksomhed skal leve op til den rolle, som er tilegnet dem samt følge vores procedurer jf. vores IT-sikkerhedspolitik samt ansvars- og rollefordeling. Dette er for at sikre, at bl.a. sikkerhedsrelaterede forhold eskaleres og håndteres. Vigtigst er, at vi passer på vores kunders data, vores udstyr og dermed vores forretning. Rolle- og ansvarsbeskrivelsen, herunder opgaver og ansvar i forhold til sikkerheden, er defineret i de udarbejdede rollebeskrivelser, medarbejdernes ansættelseskontrakt samt i IT-sikkerhedspolitikken.

Vi har procedurer for ansættelse af medarbejdere og etablering af samarbejde med eksterne, hvor vi sikrer, at vi ansætter den rigtige kandidat ift. baggrund og kompetence. Vi har rolle- og ansvarsbeskrivelser for medarbejdere og medarbejderkategorier, så alle er bekendte med deres ansvar.

Ansættelsesvilkår
Generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet. Ved ophør af en ansættelse har vi en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm, samt sikre at alle medarbejderes adgange til bygninger, systemer og data inddrages. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos adm. chefen.

Der afholdes løbende, dog minimum årligt, kurser, foredrag samt andre relevante aktiviteter til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med sikkerhed og bevidstgøres om evt. nye trusler.

Uddannelse og træning
Medarbejdere, og eksterne parter hvor det er relevant at inkludere disse under vores sikkerhedsretningslinjer, bliver periodisk orienteret om vores sikkerhedsretningslinjer, samt når der sker ændringer.

FYSISK SIKKERHED
Formål
Vi vil sikre, at vi har et betryggende fysisk miljø omkring NEM It-solutions A/S og dermed vores kunders data. Servere, services, data og informationer generelt er afskærmet mod miljømæssige påvirkninger (brand, vand, temperatur mv.), og herudover skal vi have fornøden og betryggende sikring mod hærværk, tyveri mv.

Serverrum
Vores servere er fysisk placeret i en aflåst celle i Sentias hostingcenter i Albertslund. I datacentret er der redundant køling og brandslukningsanlæg mv. Alene autoriserede personer har adgang til cellen via den etablerede procedure. Skal eksterne personer (leverandører eller kunder) have adgang til lokalet, er det i følgeskab med en af vores autoriserede medarbejdere.

Sentias køle- og brandslukningsanlæg bliver efterset periodisk, ligesom nødstrømsanlæg (UPS) halvårligt får foretaget eftersyn. Interxion har opsat systemer således, at der overvåges temperatur og strømspændinger i serverrummet.

Serverrummet indeholder vores centrale netværksudstyr, og er således sikret på samme vis som servere. Der er implementeret foranstaltninger mod tyveri, brand, vand og temperatur.
Vi modtager årligt revisorerklæring der afdækker den fysiske sikkerhed hos vores underleverandører. De seneste erklæringer er afgivet uden forbehold, eller bemærkninger af væsentlig karakter.

Kontorer
Vores kontorlokaler er monteret med tyverialarm. Ingen uvedkommende vil kunne gå uhindret omkring i vores kontorer.

Vi har etableret mulighed for, at vores medarbejdere kan arbejde hjemmefra af hensyn til bl.a. driftsvagt, og vi har politik for, at udstyr (bærbare mv.) ikke efterlades uden opsyn mv.

Bortskaffelse
Alt databærende udstyr destrueres inden bortskaffelse, for at sikre, at data ikke er tilgængeligt.

STYRING AF NETVÆRK OG DRIFT
Formål
Vi vil sikre, at vores organisering af implementering, drift og ændring i og af vores ydelse sker struktureret og efter aftale med vores kunder. Vi skal sikre at IT-sikkerheden, generelt er høj, og via systemer og procedurer til sikring heraf, ikke kompromitter vores, vores kunders systemer og data. Vi skal have procedurer for genskabelse af data, overvågning og logning af data, og vi skal generelt have opmærksomhed på fortroligheden omkring vores kunders data.

Drift
Vi vil sikre at vores drift er stabil, korrekt og sikker. Gennem løbende dokumentation og processer sikrer vi at kunne udelukke eller minimere nøglepersonsafhængighed. Opgaver tildeles og fastsættes via procedurer for styring af den operative drift.

Ændringshåndtering
Vi har defineret en proces for ændringshåndtering, for at sikre, at ændringer sker efter aftale med kunder, og er tilrettelagt hensigtsmæssigt i forhold til interne forhold. Større ændringer sker alene baseret på en klassificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer.

Ved større og/eller forretningskritiske ændringer, sikres det altid, som minimum, at;

- Alle ændringer drøftes, prioriteres og godkendes af ledelsen
- Alle ændringer testes
- Alle ændringer godkendes før idriftsættelse
- Alle ændringer idriftsættes på et fastsat tidspunkt, efter aftale med forretningen og/eller kunden
- Der fortages fall back-planlægning, som sikrer, at ændringer kan rulles tilbage eller annulleres, hvis den ikke fungerer
- Systemdokumentationen opdateres med den nye ændring, såfremt det vurderes nødvendigt

Vores miljø, kan efter behov, opdeles logisk, i test og produktion, hvorved vi sikrer at have testet et produkt eller ændring, før den kommer i produktion. Via den indbyggede adgangsstyring i RDM-værktøjet, sikrer vi at kun autoriseret personale har adgang til dette.

Log-oplysninger
Vi beskytter vores log-oplysninger mod manipulation og uautoriseret adgang. System og operatørlogge opsamles fra udstyr som vedrører drift og opbevares på 2 af hinanden uafhængige lagersystemer.

Tidssynkronisering
Vi har sikret at urene i vores informationsbehandlingssystemer er synkroniseret og har samme tids stempel. Dette har betydning i tilfælde af informationssikkerhedshændelser hvor logs fra forskellige systemer skal gennemgås.

Afhængighed af nøglepersoner
Selvom vores organisation ikke nødvendigvis gør, at vi kan have overlap inden for alle opgaver og systemer, sikrer vi via dokumentation og beskrivelser - og via kompetente og flittige medarbejdere - at medarbejdere eller nye medarbejdere kan påbegynde et arbejde på et system, som vedkommende ikke har operationel og historisk erfaring med.

Underleverandører
Hvor vi bruger underleverandører fører vi tilsyn med de aftalte leverancer, idet disse skal efterleve vores egne politikker for ydelseslevering, herunder vores forretningsvilkår med vores kunder.

Kapacitet og systemtest
Via vores overvågningssystem, har vi sat grænseværdier for hvornår vores overordnede systemer, og dermed vores kunders systemer, skal skaleres op af hensyn til elektronisk plads, svartider mv. Når vi opsætter nye systemer foretages test af funktionalitet og herunder kapacitet- og performancetest.

Skadevoldende kode
Vi har implementeret scannings- og overvågningssystemer til at sikre mod kendt skadevoldende kode, dvs. hvad vi og vores kunder - via vores platforme - kan risikere at blive inficeret med på internettet, via e-mails mv. Vi har antivirus-systemer, systemer til overvågning af internetbrug, trafik og ressourcer på RDP-platforme, samt sikringer i øvrige tekniske og centrale installationer (firewall mv.).

Sikkerhedskopiering
Vi sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis, samt efter de aftaler, vi har med vores kunder.

Vi har etableret en testplan for verificering af hvorvidt sikkerhedskopieringen fungerer samt en test af hvordan systemer og data praktisk kan reetableres. Der føres en log over disse tests, således at vi kan følge op på om vi kan ændre på procedurer og processer for at højne vores løsning.

Medmindre andet er aftalt med vores kunder, foretager vi sikkerhedskopiering af hele deres virtuelle miljø hos os. Vi foretager sikkerhedskopiering af vores egne systemer og data på samme vis, som vores kunders systemer og data.

Vi har defineret retningslinjer for på hvilken vis, vi foretager sikkerhedskopiering. Hver nat føres udvalgte data fra vores centrale systemer til vores colocation ved hjælp af vores backup-system. Dermed er data fysisk separeret fra vores driftssystemer, og efter endt afvikling, foretages der en automatiseret verificering af, hvorvidt datamængde og indhold mellem vores driftssystem og colocation, stemmer overens.

En ansvarlig medarbejder sikrer herefter, at sikkerhedskopieringen er sket, foretager det fornødne hvis jobbet er fejlet, og logfører herefter dette.

Netværkssikkerhed
IT-sikkerheden omkring systemers og datas ydre rammer, er netværket mod internettet, remote eller lignende. Vi mener at have sikret data og systemer også inde i netværket, men det ydre værn mod uvedkommende adgang, er af højeste prioritet hos os.

Adgang til vores systemer fra vores kunder, sker enten via de offentlige netværk, hvor adgang sker via en krypteret RDP-adgang.

Alene godkendt netværkstrafik (indgående) kommer gennem vores firewall.

Vi er ansvarlige for driften og sikkerheden hos os, dvs. fra og med systemerne hos os og ud til internettet. Vores kunder er selv ansvarlige for at kunne tilgå internettet.

Håndtering af databærende medier
Vi sikrer, i bedst muligt omfang, at vores medarbejderes bærbare medier såsom bærbare pc'er, smartphones, tablets og lign. er konfigureret sikkerhedsmæssigt lige så højt, som resten af vores miljø, samt det sikres at de databærende medier opdateres når vi foretager nye sikkerhedstiltag.

Vi skal sikre, at vores og vores kunders systemer og data beskyttes. Vi håndterer derfor ikke kunders data på håndbårne medier (Eksterne USB-medier, CD/DVD) uden forudgående skriftlig aftale med kunderne samt ved passende fysisk beskyttelse mod miljømæssige på- virkninger (varme mv.) samt hærværk og tyveri.

Alt databærende udstyr (USB, SSD, harddiske mv.) destrueres inden bortskaffelse for at sikre, at data ikke

er tilgængeligt.

Vores dokumentation opbevares på to af hinanden uafhængige lokationer. Dette sikrer tilgængeligheden af dokumentationen i tilfælde af f.eks. nedbrud.

Ekstern datakommunikation
Ekstern datakommunikation sker alene via e-mails, idet vores kunders adgang og brug af vores servere, ikke betragtes som ekstern datakommunikation.

Glemte kodeord, personoplysninger, bestillinger mv. håndteres aldrig via telefon, udelukkende på skrift (opdelt på e-mail og SMS) og først efter vores medarbejdere har konstateret, at det er den korrekte og autoriserede person, vi har kontakt til.

Aftaler om informationsoverførsel
Vi har indgået aftaler om informationsoverførsel med vores kunder og leverandører. Dette sikrer at gældende lovgivning overholdes og at samarbejdet er formaliseret.

Overvågning og logning
Vi har et overvågningssystem hvor vi overvåger driftskritiske servere og udstyr. Vores driftsmedarbejdere foretager den daglige overvågning af vores systemer via måling af grænseværdier. Vi opsamler logs for alle servere og enheder i netværket.

Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident og problem management procedurer til sikring af, at hændelser registreres, prioriteres, styres, eskaleres og at der foretages de nødvendige handlinger.

ADGANGSSTYRING
Formål
Vi vil sikre, at vores og vores kunders adgange ske efter hensigten, og at det alene er personer med autoriseret adgangsniveau, der har adgang til data. Vi vil sikre, at der er sporbarhed i brugen af systemer og data, og adgangen sker IT-sikkerhedsmæssigt betryggende.

Vi har defineret en række retningslinjer og procedurer herfor.

Brugeroprettelse og nedlæggelse
Vores kunders brugere oprettes alene på baggrund af vores kunders ønske. Vores kunder er dermed ansvarlige herfor og for nedlæggelse. Vores egne brugere oprettes alene på baggrund af skriftligt ønske fra ledelsen.

Alle brugere skal være personhenførbare, dvs. have tydeligt mærke med personnavn. Er der tale om servicebrugere, altså konti som alene benyttes systemmæssigt, er muligheden for at egentlig logon deaktiveres.

Kodeord
Alle brugere på tværs af både kundesystemer og egne systemer, har restriktioner omkring adgangskode. Alle brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger ift. udformningen af kodeordet. Koder skal skiftes regelmæssigt og være komplekse.

Vores IT-sikkerhedspolitik beskriver, at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet.

Gennemgang af brugere
For vores egne brugere, gennemgår ledelsen periodisk, minimum årligt, en liste med oprettede brugere og deres adgangsniveau for at sikre mod adgang for uautoriserede personer.

Brugeradgang til data
Vores medarbejdere er opsat med differentieret adgang, og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen. Vi anvender et system til styring af privilegerede adgangsrettigheder, som sikrer at medarbejdernes adgang til kundernes systemer logges individuelt.

Vores kunders brugeradgange til kundens systemer og data, bestemmes af vores kunder.

Skærmlås
Hvis der ikke har været input på sessionen i en periode på 45 minutter, disconnectes medarbejderen automatisk.
Computere skal ligeledes slukkes inden arbejdspladsen forlades, samt altid være beskyttet af password.

Adgangsveje til netværk og netværksudstyr
Vores netværk er komplekst med mange systemer og kunder. For at sikre os mod at uvedkommende får adgang, og for at sikre gennemskueligheden af opbygningen, har vi udformet en dokumentation, der beskriver det interne netværk med enheder, navngivning af enheder, logisk opdeling af netværk mv. Dokumenterne, netværkstopologier og lign. opdateres løbende ved ændringer.

Adgangsmuligheder (logon, vpn)
Adgang til vores netværk og dermed potentielt til systemer og data, skal ske for kun autoriserede personer.

Adgang udenfor vores interne netværk, kan ske på forskellig vis som afhænger af den enkelte aftale med kunden. Der er mulighed for at logge på via krypteret RDP-forbindelse eller via VPN. I begge tilfælde skal der benyttes brugernavn og kode for at logge på. NEM medarbejdere kan kun logge på vores systemer via RDP med 2-faktor autentifikation.

Styring af adgangskoder
Da vi har brugere, såsom service accounts og lign, som ikke kan bruges til at logge på med, og af systemmæssige årsager ikke skifter passwords, har vi et system til opbevaring af disse passwords. Kun autoriseret personale har adgang til systemet.

Adgang til systemer og data via mobile enheder
Vi har åbnet adgang for, at vi kan benytte mobile enheder (smartphones, tablets mv.) til synkronisering af e-mails og kalender. Ud over kode, har vi ikke implementeret andre sikkerhedsforanstaltninger til sikring af disse enheder og disses brugeradgange.

Vores kunder har mulighed for det samme, og det er op til vores kunder at implementere deres IT-sikkerhedspolitik for deres brugere.

Inddragelse af adgangsrettigheder
Vi har en klart defineret politik og procedure for inddragelse af adgangskontrol ved ændringer i ansættelsesforhold, f.eks. i forbindelse med afskedigelse af en medarbejder. Proceduren inkluderer også inddragelse af adgang til vores Hostingfaciliteter.

STYRING AF SIKKERHEDSHÆNDELSER
Formål
Håndtering af sikkerhedshændelser tager vi meget alvorligt. Vi definerer sikkerhedshændelser bredt, og har procedurer for håndtering af hændelser, såsom opdateringer af patches, virusinficerede filer og systemer, overvågning for hackerangreb mv. for at sikre, at vi beskytter vores og vores kunders systemer og data bedst muligt.

Rapportering af sikkerhedshændelser
Vi har udarbejdet procedurer for håndtering sikkerhedshændelser og rapportering af disse. Sikkerheds-

hændelser afstedkommet fra hhv. egne observationer, alarmering ud fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, blive eskaleret til vores tekniske afdeling med samtidig orientering til ledelsen.

Vores medarbejdere og eksterne samarbejdspartnere er, via de indgåede kontrakter og aftaler, forpligtet til at anmeldelse enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelsen, og nødvendige tiltag kan udføres jf. de etablerede procedurer.

Vi holder os fagligt opdaterede vha. producenters supporthjemmesider, debatfora mv. for konstaterede svagheder i de systemer, vi benytter og tilbyder.

Håndtering af sikkerhedshændelser
Opstår en hændelse, er det den enkelte medarbejder der vurderer hvilken reaktion der skal ske. Herefter foretages det fornødne, for at orientere kunder og omverden og udbedre forholdet. Dette sker efter konsultation af ledelse eller kollegaer.

Sker en hændelse inden for normal arbejdstid, vil NEM NOC håndtere og eskalere sagen på samme vis som andre sager, og med den prioritering som er nødvendig. Til styring af overvågning og opfølgning på hændelser, har vi implementeret formelle incident- og problem management procedurer, til sikring af, at hændelser registreres, prioriteres, styres, eskaleres, og at der foretages de nødvendige handlinger. Forløbet dokumenteres i ticketsystemet.

Opdateringer installeres ugentligt, eller minimum 1 gang pr. måned. Både Windows systemer og 3. parts applikationer opdateres.

Evaluering af sikkerhedshændelser
En sikkerhedshændelse kan - afhængig af forholdet - blive genstand for efterfølgende efterforskning. Dette kan ske internt af hensyn til evaluering, og eventuel ændring i procedurer, tekniske eller logiske forhold. Det er også muligt, at der ved kriminelle forhold skal ske en politimæssig efterforskning. I alle tilfælde vil vores logføring og øvrige overvågningssystemer, kunne benyttes til at evaluere på sikkerhedshændelsen.

Udover evalueringen foretager vi en root cause analyse for at sikre, at de opståede sikkerhedshændelser ikke gentager sig.

BEREDSKABSPLAN
Formål
Vi vil have mulighed for at genoptagelse af vores primære og centrale forretningsprocesser og systemer, efter en katastrofelignende situation.

Beredskabsplan
Skulle der opstå en nødsituation, har NEM It-solutions A/S udarbejdet en overordnet beredskabsplan. Beredskabsplanen er forankret i IT-risikoanalysen og vedligeholdes minimum årligt, i forlængelse af udførelsen af analysen. Planen testes 1 gang årligt som en del af vores overordnet beredskab, så vi sikrer, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften, i forbindelse med en eventuel nødsituation.

Planen og procedurerne er forankret i vores driftsdokumentation og procedurer.

OVERENSSTEMMELSE MED LOVBESTEMTE OG KONTRAKTLIGE KRAV
Vi er ikke underlagt særlig lovgivning i forhold til vores ydelse. Vores kunder kan dog være, og de steder, er vores understøttelse heraf aftalt særskilt.

Vi lader os årligt revidere af ekstern revisor, med henblik på afgivelse af erklæring for overholdelsen af kontrollerne, nævnt i denne beskrivelse.

Vi har en intern kontrol, hvor vi undersøger, om de etablerede politikker og retnings- linjer overholdes af medarbejderne. Derudover har vi en kontrol der sikrer, at vores udstyr, såsom servere, databaser, net-værksudstyr mm., er sat op jf. vores baselines.

ÆNDRINGER I PERIODEN FRA 1.1.2021 TIL 31.12.2021

Vi har ikke foretaget væsentlige ændringer i hostingydelser og de tilhørende tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller i perioden 1. januar til 31. december 2021.

KOMPLEMENTERENDE KONTROLLER

NEM It-solutions A/S kunder er, medmindre andet er aftalt, ansvarlige for at etablere forbindelse til NEM It-solutions A/S servere. Herudover er NEM It-solutions A/S kunder, medmindre andet er aftalt, ansvarlige for:

- at det aftalte niveau for backup dækker kundens behov.
- periodisk gennemgang af kundens egne brugere.

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 NEM IT-Solutions beskrivelse Hostingplatformen 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 NEM It-solutions, 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. januar til 31. december 2021.

Udførte testhandlinger

Test af udformningen af tekniske og organisatoriske sikkerhedsforanstaltninger og øvrige kontroller samt implementeringen og effektiviteten 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.

For de ydelser, som Sentia A/S leverer inden for it-hosting, har vi modtaget en ISAE 3402 type erklæring for perioden 1 januar til 31. december 2021 vedrørende serviceunderleverandørens kontroller.

Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i NEM IT-solutions beskrivelse af Hostingplatformen og de tilhørende kontroller. Vi har således alene inspiceret den modtagne dokumentation og testet de kontroller hos NEM It-solutions, der sikrer overvågning af serviceunderleverandørens opfyldelse af den mellem serviceunderleverandøren og NEM It-solutions 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.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed

- *At give retningslinjer for og understøtte informationssikkerheden, herunder at informationssikkerhedspolitikker er godkendt, informere og ajourført.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
5.1.1 Politikker for informationssikkerhed ▶ Serviceleverandøren foretager løbende risikovurdering samt, når serviceleverandøren foretager ændringer eller implementerer nye systemer, som vurderes relevante i forhold til at revurdere den generelle risikovurdering. ▶ Serviceleverandøren har definereret en informationssikkerhedspolitik, som er gældende for medarbejdere og ledelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politikken for risikovurdering og observeret at der er foretaget en samlet risikovurdering af systemer og services. Vi har ved forespørgsels fået oplyst, at proceduren er gennemgået i december 2021 sammen med risikoanalysen. Vi har inspiceret politikker for informationssikkerhed og understøttende procedurebeskrivelser og observeret, at der er udarbejdet en opdateret og ledelsesgodkendt informationssikkerhedspolitik. Vi har inspiceret adgang til mappen med informationssikkerhedspolitikken og observeret, at medarbejderne har adgang til mappen.	Ingen afvigelser konstateret
5.1.2 Gennemgang af politikker for informationssikkerhed ▶ Serviceleverandøren skal sikre, at politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer, for at sikre deres forsatte egnethed, tilstrækkelighed og effektivitet. ▶ Serviceleverandørens informationssikkerhedspolitikker skal gennemgås minimum 1 gang årligt eller ved væsentlige ændringer.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret NEM It-Solutions årshjul og observeret, at der heraf fremgår, at informationssikkerheden skal gennemgås kvartalsvist, og vi har inspiceret understøttende dokumentation for de kvartalsvise inspektioner. Vi har inspiceret dokumentation for gennemgang af informationssikkerhedspolitikken og observeret, at den er blevet gennemgået november 2021.	Ingen afvigelser konstateret

A.6 Organisering af informationssikkerhed

Kontrolmål 6.1 – intern organisering

- *At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.6.1.1 Roller og ansvarsområder for informationssikkerhed - Serviceleverandøren har etableret en intern it-sikkerhedsorganisation, som sikrer, at politikker og procedurer ajourføres og bidrager til optimering af det aktuelle sikkerhedsniveau hos serviceleverandøren. - Serviceleverandørens it-sikkerhedsorganisation afholder faste møder hvert kvartal og ellers efter behov	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret informationssikkerhedspolitikker og har observeret, at der er udpeget en informationssikkerhedsorganisation med ansvar for politikker og procedurer. Vi har for en stikprøve inspiceret dokumentation for at it-sikkerhedsorganisation har afholdt kvartalsvise møder i 2021.	Ingen afvigelser konstateret
A.6.1.2 Funktionsadskillelse - Serviceleverandøren skal sikre, at samme person ikke har adgang til at tilgå, ændre og anvende systemer, informationer eller infrastruktur, uden at dette er godkendt eller vil blive opdaget. - Serviceleverandøren har en klar opdelt organisation i forhold til informationssikkerhed og har udførlige ansvars- og rollebeskrivelser for de enkelte medarbejdere.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens rollebeskrivelser og observeret, at ansattes adgange er begrænsede i forhold til den rolle de besidder i virksomheden. Vi har inspiceret dokumentation for kvartalsvis gennemgang af brugers rettigheder til kunders systemer.	Ingen afvigelser konstateret
A.6.1.5 Informationssikkerhed ved projektstyring - I forbindelse med afsluttede og igangværende projekter, skal det kontrolleres, at der er/har været udpeget en projektansvarlig, at der er gennemført risikovurdering af projektet, at det er planlagt og koordineret sammen med kunden og at projektet regelmæssigt er gennemgået eller gennemgås i forhold til informationssikkerhed.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politik for informationssikkerhed ved projektstyring. Vi har for gennemførte projekter i erklæringsperioden inspiceret dokumentation i form af en ticket på service request, hvoraf risikovurdering, projektansvarlig mv. er anført i henhold til politikken.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

Kontrolmål 6.2 – Mobilt udstyr og fjernarbejdspladser

- *At sikre fjernarbejdspladser og brugen af mobilt udstyr*

Kontrolaktivitet	Test udført af BDO	Resultat af test
A.6.2.1 Politik for mobilt udstyr ▶ Serviceleverandøren har udformet og implementeret politik for anvendelse af mobile enheder. ▶ Serviceleverandørens mobile enheder er beskyttet af adgangskode.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politik for mobilt udstyr og politik for brug af mobilt udstyr og observeret, at der heraf fremgår regler for anvendelse af mobile enheder samt krav om beskyttelse af dem via adgangskoder. Vi har for tre stikprøve udvalgte ansatte observeret, at disse efterlever politikken for brug af mobiltudstyr.	Ingen afvigelser konstateret
A.6.2.2 Fjernarbejdspladser ▶ Serviceleverandøren har ved anvendelse af fjernarbejdspladser defineret, at udstyr ikke må efterlades uden opsyn. ▶ Serviceleverandøren anvender to-faktor godkendelse ved login via fjernadgang.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for fjernadgang, og observeret medarbejderne skal logge ind med to-faktor godkendelse. Vi har observeret medarbejders login fra eksternt netværk og observeret, at to-faktor godkendelse anvendes for at tilgå netværket.	Ingen afvigelser konstateret

A.7 Personalesikkerhed

Kontrolmål 7.1. - Før ansættelsen

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
7.1.1 Screening ▶ Serviceleverandøren har procedurer for ansættelse af medarbejdere og etablering af samarbejde med eksterne. ▶ Serviceleverandøren gennemfører en screening ud fra en individuel vurdering i forhold til ansættelse eller samarbejdsforholdet.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for ansættelser og observeret at den definerer at nye medarbejders CV, uddannelsesbevis og gyldig legitimation skal indhentes inden start. Vi har ved forespørgsel fået oplyst, at der ikke har været ansættelser i erklæringsperioden, hvorfor vi ikke har kunne verificere, at proceduren er blevet efterlevet i erklæringsperioden.	Ingen afvigelser konstateret.
7.1.2 Ansættelsesvilkår- og betingelser ▶ Serviceleverandørens generelle vilkår for ansættelse, herunder fortrolighed om egne og kunders forhold, er beskrevet i hver medarbejders ansættelseskontrakt, hvor forhold omkring alle sider af ansættelsen, herunder ophør og sanktioner ved evt. sikkerhedsbrud, er angivet.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for ansættelsesvilkår og observeret, at medarbejder skal underskrive en fortrolighedsaftale. Vi har inspiceret serviceleverandørens standardansættelseskontrakt og observeret, at denne beskriver alle sider af ansættelsen. Vi har ved forespørgsel fået oplyst, at der ikke har været ansættelser i erklæringsperioden, hvorfor vi ikke har kunne verificere, at proceduren er blevet efterlevet i erklæringsperioden.	Ingen afvigelser konstateret.

A.7 Personalesikkerhed

Kontrolmål 7.2 – Under ansættelsen

- *At sikre medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
7.2.1 Ledelsesansvar ▶ Serviceleverandøren skal undervise alle medarbejdere i informationssikkerhed.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for ledelsesansvar og observeret, at der heri er anført, at ledelsen skal undervise alle medarbejdere i informationssikkerhed. Vi har inspiceret dokumentation for den afholdte træning i erklæringsperioden og observeret, at træningen omfattede emner om informationssikkerhed samt at alle medarbejder har været igennem denne træning.	Ingen afvigelser konstateret.
7.2.2 Bevidsthed om, uddannelse og træning i informationssikkerhed ▶ Serviceleverandøren afholder løbende, dog mindst en gang årligt, kurser, foredrag samt andre relevante aktiviteter til sikring af, at relevante medarbejdere og evt. eksterne samarbejdspartnere holdes ajour med sikkerhed og bevidstgøres om evt. nye trusler.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret dokumentation for den afholdte træning i erklæringsperioden og observeret, at træningen omfattede emner om informationssikkerhed samt at alle medarbejder har været igennem denne træning.	Ingen afvigelser konstateret.
7.2.3 Sanktioner ▶ Serviceleverandøren har opstillet regler for sanktioner.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret databehandlerens standard ansættelseskontrakt og observeret, at denne indeholder en henvisning til databehandlerens medarbejderhåndbog hvori reglerne for sanktioner fremgår. Vi er ved forespørgsel blevet informeret om, at ingen ansatte er blevet pålagt sanktioner, hvorfor vi ikke har kunne verificere effektiviteten af reglerne.	Ingen afvigelser konstateret.

A.7 Personalesikkerhed

Kontrolmål 7.3 – Ansættelsesforholdets ophør eller ændring

- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
7.3.1 Ansættelsesforholdets ophør eller ændring ▶ Serviceleverandøren har ved ophør af en ansættelse en udførlig procedure, som skal følges, for at sikre, at medarbejderne indleverer alle relevante aktiver, herunder bærbare medier mm, samt sikre at alle medarbejderes adgange til bygninger, systemer og data inddrages. ▶ Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos administrationschefen.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedure for fratrædelse og observeret, at medarbejder skal tilbagelevere alt udstyr ved ophør og kvittere for tilbageleveringen. Vi har ved forespørgsel fået oplyst, at der ikke har været ophør af ansættelsesforhold i erklæringsperioden, hvorfor vi ikke har kunne verificere, at proceduren er blevet efterlevet i erklæringsperioden.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

Kontrolmål 8.1 – Ansvar for aktiver

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
8.1.1 Fortegnelse over aktiver ▶ Serviceleverandøren fører fortegnelse over aktiver til brug ved dokumentation, overblik over udstyr mv.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret oversigten over aktiver og observeret, at der er tildelt en systemejer for alle aktiver. Vi har inspicereret oversigt over aktiver i systemet og observeret, at de ajourføres via ticket-systemet. Vi har stikprøvevis inspiceret dokumentation på kundeniveau for at oversigten med aktiver er blevet opdateret i erklæringsperioden.	Ingen afvigelser konstateret.
8.1.2 Ejerskab af aktiver ▶ Serviceleverandøren har ansvarsfordeling og rollebeskrivelser for centrale netværksenheder, servere, periferienheder, systemer og data tilegnet systemansvarlige. ▶ Serviceleverandøren arbejder med ejerskab for at sikre, at ingen enheder, systemer eller data bliver glemt i forhold til sikkerhedsopdatering, klassifikation, drift og vedligeholdelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politikken for ejerskab af aktiver og observeret, at der er foretaget en ansvarsfordeling over aktiver, baseret på den organisatoriske rolle. Vi har inspicereret serviceleverandørens miljø og har herfra observeret, at den tekniske organisation har ansvaret for aktivet.	Ingen afvigelser konstateret.
8.1.3 Accepteret brug af aktiver ▶ Serviceleverandørens Informationssikkerhedspolitik fastsætter rammerne for medarbejdernes anvendelse af serviceleverandørens informationssystemer og aktiver.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret informationssikkerhedspolitikken og medarbejder håndbogen og observeret, at der heri er angivet regler for medarbejdernes benyttelse af aktiverne.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

Kontrolmål 8.1 – Ansvar for aktiver

- *At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
8.1.4 Tilbagelevering af aktiver ▶ Serviceleverandørens medarbejdere tilbageleverer alt udleveret udstyr ved fratrædelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret proceduren for fratrædelse af medarbejdere og observeret, at der heri er anført, at medarbejdere skal kvittere for at have tilbageleveret udstyr ved fratrædelse. Vi er ved forespørgsels blevet informeret om, at der ikke har været fratrædelser i erklæringsperioden, hvorfor vi ikke har kunne efterprøve kontrollen i erklæringsperioden.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

Kontrolmål 8.2 – Ansvar for aktiver

- *At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
8.2.1 Klassifikation af information ▶ Serviceleverandøren har udarbejdet en politik for klassifikation af informationer. ▶ Kun serviceleverandørens betroede medarbejdere, som har underskrevet en tavshedserklæring, har adgang til systemer og service med kundedata. ▶ Serviceleverandøren har dokumenteret udstyr og service, som indeholder kundedata.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for klassifikation af information og observeret, at der forelægger procedurer for klassifikation af kundedata. Vi har for en stikprøve udvalgt medarbejder observeret, at medarbejderens ansættelseskontrakt indeholdt et afsnit om tavshedspligt. Vi har inspicereret stikprøve udvalgt servere og observeret, at der forelægger dokumentation for klassifikation af kundedata på serverne.	Ingen afvigelser konstateret.
8.2.2 Mærkning af information ▶ Al kundedata hos serviceleverandøren er mærket fortrolig.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret oversigt over informationer på kunder og observeret, at alle informationer indeholdende kundedata er mærket som fortrolig. Vi har inspicereret en stikprøve udvalgt kundeserver og observeret, at data i serveren er markeret som værende fortroligt.	Ingen afvigelser konstateret.
8.2.3 Håndtering af aktiver ▶ Serviceleverandøren har angivet regler for håndtering af aktiver. ▶ Serviceleverandørens medarbejdere er bekendt med håndtering og behandling af aktiver.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for håndtering af aktiver og observeret, at medarbejdere håndterer informationer og aktiver ud fra deres rolle hos serviceleverandøren, og at den enkelte medarbejder er bekendt med informationer og aktiver jf. informationssikkerhedspolitikken.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

Kontrolmål 8.2 – Ansvar for aktiver

- *At sikre passende beskyttelse af information, der står i forhold til informationens betydning for organisationen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspicereret medarbejdernes roller og har ved forespørgsel af udvalgte medarbejdere konstateret, at de er bekendt med serviceleverandørens regler for håndtering og behandling af aktiver.	

A.8 Styring af aktiver

Kontrolmål 8.3 – Mediehåndtering

- *At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
8.3.1 Styring af bærbare medier ▶ Serviceleverandøren sikrer, at medarbejderes bærbare medier, såsom bærbare pc'er, smartphones, tablets og lign., er konfigureret sikkerhedsmæssigt.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret procedure for styring af bærbare medier. Vi har inspicereret konfigurationen for et bærbart medie og observeret, at det opdateres automatisk.	Ingen afvigelser konstateret.
8.3.2 Bortskaffelse af medier ▶ Serviceleverandøren destruerer alt databærende udstyr, inden bortskaffelse for at sikre, at data ikke er tilgængeligt.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for bortskaffelse af medier og observeret, at der heri er anført, alt databærende udstyr skal destrueres af et af serviceleverandøren godkendt eksternt firma. Vi har inspiceret dokumentation for, at destrueret udstyr i erklæringsperioden er blevet destrueret i overensstemmelse med proceduren.	Ingen afvigelser konstateret.
8.3.3 Fysiske medier under transport ▶ Serviceleverandøren har defineret en politik for, at sikre medier, der indeholder data klassificereret som fortroligt eller til intern, kun sendes med en godkendt transportør.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedurer for transport af fysiske medier og observeret, at der heri er anført, at alt databærende udstyr skal transporteres af en godkendt transportør. Vi har for transporter i erklæringsperioden inspiceret dokumentation for, at der er anvendt en godkendt transportør til opgaven samt at mediet er sikret ved password.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål 9.1 – Forretningsmæssige krav til adgangsstyring

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
9.1.1 Politik for adgangsstyring ▶ Serviceleverandørens kunders adgange skal ske efter hensigten, og alene personer med autoriseret adgangsniveau har adgang til data. ▶ Serviceleverandøren skal sikre, at der er sporbarhed i brugen af systemer og data, og at adgangen sker it-sikkerhedsmæssigt betryggende. ▶ Serviceleverandøren har defineret en række retningslinjer og procedurer herfor.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politikken for adgangsstyring og observeret, at den er opdateret og ledelsesgodkendt. Vi har inspiceret roller og tildelte adgangsrettigheder, og observeret at medarbejderne har fået tildelt rollebaseret adgang til systemerne. Vi har inspiceret aktivitetslogen og observeret, at det på kundeniveau er muligt at have sporbarhed over brugen af systemerne. Vi har observeret, at der er ført kvartalsmæssig kontrol med at kunders adgange er sikre.	Ingen afvigelser konstateret.
9.1.2 Adgang til netværk og netværkstjenester ▶ Serviceleverandøren tildeler adgang til Windows Active Directory efter ledelsesgodkendelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret procedure for adgang til netværk og netværkstjenester og observeret, at serviceleverandøren skal tildele adgang efter ledelsesgodkendelse. Vi er ved forespørgsel blevet oplyst, at der ikke er oprettet nye egne brugere i erklæringsperioden, hvorfor vi ikke har kunne efterprøve hvorvidt adgang til Windows Active Directory sker efter ledelsesgodkendelse.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål 9.2 – Administration af brugeradgang

- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
9.2.1 Brugerregistrering og -afmelding ▶ Serviceleverandørens kunders brugere oprettes alene på baggrund af kunders ønske, hvorved kunderne er ansvarlige herfor og for nedlæggelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for systemadgang for medarbejdere, kontrahenter og kunder og observeret, at der heri er anført, at kunder skal oprettes efter, at der er blevet indsendt en forespørgsel fra kontaktperson hos kunden. Vi har ved stikprøve inspiceret dokumentation for at brugere er blevet oprettet i overensstemmelse med den relevante procedure.	Ingen afvigelser konstateret.
9.2.2 Tildeling af brugeradgang ▶ Serviceleverandøren opretter egne brugere på baggrund af skriftlig ledelsesgodkendelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politikken for brugerregistrering og -afmelding, og observeret at der heri er anført at oprettelse, nedlæggelse samt ændring af brugerrettigheder for medarbejdere, kun må foretages efter godkendelse af ledelsen. Vi har ved forespørgsel fået oplyst, at der ikke er oprettet nye egne brugere i erklæringsperioden, hvorfor vi ikke har kunne verificere, at proceduren er blevet efterlevet i erklæringsperioden. Vi har inspicereret tildelte adgange i Windows Active Directory, og observeret, at der er tildelt adgange til medarbejdere med et arbejdsbetinget behov.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål 9.2 – Administration af brugeradgang

- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
9.2.3 Styring af privilegerede adgangsrettigheder ▶ Serviceleverandørens tildeling og anvendelse af privilegerede adgangsrettigheder begrænses til brugere med et arbejdsbetinget behov.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for styring af privilegerede adgangsrettigheder, og observeret adgang sker gennem remote desktop manager. Vi har inspicereret oprettede medarbejdere i Windows Active Directory med administratorrettigheder og observeret, at systemadministratoradgange er tildelt efter et arbejdsbetinget behov. Vi har inspicereret periodisk gennemgang af privilegerede rettigheder og observeret, at ledelsen har gennemgået rettighederne.	Ingen afvigelser konstateret.
9.2.4 Styring af hemmelig autentifikationsinformation om brugere ▶ Serviceleverandøren foretager autorisation af kunde før udstedelse af nyt kodeord. ▶ Serviceleverandørens kunder kan alene bestille nye kodeord på enten e-mail eller SMS.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedure for identifikation af brugere ved udlevering af nyt password og observeret, at det heri fremgår at serviceleverandøren foretager autorisation af kunden før nyt kodeord udstedes samt at udstedelsen skal ske via enten e-mail eller sms. Vi har ved stikprøve inspicereret bestilling af nyt password fra kunde og observeret, at bestillingen blev telefonisk verificeret, før der efterfølgende blev sendt adgangskode via SMS.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål 9.2 – Administration af brugeradgang

- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
9.2.5 Gennemgang af brugeradgangsrettigheder ▶ Serviceleverandørens foretager en kvartalsvis gennemgang af brugere og tildelte brugerrettigheder.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret årshjulet, og observeret at der skal foretages en kvartalsvis gennemgang af tildelte adgangsrettigheder for brugere hos serviceleverandøren. Vi har inspiceret dokumentation for den kvartalsvise gennemgang af brugere er foretaget	Ingen afvigelser konstateret.
9.2.6 Inddragelse eller justering af adgangsrettigheder ▶ Ved ændringer i ansættelsesforhold, afskedigelse af en medarbejder eller ophør af kontrakt m.m., inddrager serviceleverandøren adgangen.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedure for nedlukning af brugere og observeret, at serviceleverandøren skal inddrage adgangsrettigheder ved ændringer i ansættelsesforhold, afskedigelse af medarbejder eller ved ophør af kontrakter. Vi har ved forespørgsel fået oplyst, at der ikke har været inddragelse eller justering af adgangsrettigheder i erklæringsperioden, hvorfor vi ikke har kunne verificere, at proceduren er blevet efterlevet i erklæringsperioden.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål 9.3 – Brugernes ansvar

- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation*

Kontrolaktivitet	Test udført af BDO	Resultat af test
9.3.1 Brug af hemmelig autentifikationsinformation ▶ Serviceleverandørens brugere har på tværs af både kundesystemer og egne systemer restriktioner omkring adgangskode. ▶ Serviceleverandørens brugere har en adgangskode, og det er systemmæssigt sat op således, at der er begrænsninger ift. udformningen af kodeordet. ▶ Koder skal skiftes regelmæssigt og være komplekse.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret passwordpolitikken og observeret, at kompleksitet skal være aktiv, og at kodeordet skal skiftes regelmæssigt. Vi har inspicereret Default Domain Policy og observeret, at passwordpolitikken heri er i overensstemmelse med passwordpolitikken for brugeren jf. informationssikkerhedspolitikken.	Ingen afvigelser konstateret.

A.9 Adgangsstyring

Kontrolmål 9.4 – Styring af system- og applikationsadgang
- *At forhindre uautoriseret adgang til systemer og applikationer*

Kontrolaktivitet	Test udført af BDO	Resultat af test
9.4.1 Begrænset adgang til information ▶ Serviceleverandørens medarbejdere er opsat med differentieret adgang og har således alene adgang til de systemer og til de data, som er relevant for arbejdsindsatsen.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for begrænsning af adgang til systemer og applikationer og observeret, at denne anfører at medarbejdere skal tildeles adgange, basereret på roller og ansvar. Vi har inspicereret Microsoft Active Directory og observeret, at brugere er tildelt adgange, basereret på deres roller og ansvar i organisationen.	Ingen afvigelser konstateret.
9.4.2 Procedurer for sikkert log-on ▶ Serviceleverandørens medarbejdere kan kun logge på systemerne via RDP med to-faktor autentifikation.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for sikkert log-on og observeret, at der forelægger retningslinjer for tildeling af adgange til systemer og applikationer. Vi har observeret, at serviceleverandørens medarbejdere skal logge ind med to-faktor autentifikation.	Ingen afvigelser konstateret.
9.4.3 System for administration af adgangskoder ▶ Serviceleverandørens brugere, såsom service accounts og lign, som ikke kan bruges til at logge på med, og af systemmæssige årsager ikke skifter passwords, har et system til opbevaring af disse passwords. ▶ Kun serviceleverandørens autoriseret personale har adgang til systemet.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret opbevaring af adgangskoder for servicebrugere og inspiceret serviceleverandørens kontrol af at kun autoriseret personale har adgang til disse.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

Kontrolmål 11.1 – Sikre områder

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
11.1.1 Fysisk perimetersikring ▶ Serviceleverandørens servere er fysisk placeret i en aflåst celle i Sentias' hostingcenter i Albertslund. I datacentret er der redundant køling og brandslukningsanlæg mv. ▶ Serviceleverandøren modtager årligt revisorerklæring der afdækker den fysiske sikkerhed hos underleverandører. ▶ Serviceleverandøren gennemgår og vurderer årligt revisorerklæring.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret ISAE 3402 erklæring for periode 1. januar til 31. december 2021 fra uafhængig revisor for Sentia A/S og observeret, at fysisk sikkerhed er blevet gennemgået, og der ikke forelægger bemærkninger. Vi har inspicereret serviceleverandørens kontrol af revisorerklæring fra Sentia A/S og observeret, at serviceleverandøren har gennemgået og vurderet revisorerklæringen uden bemærkninger.	Ingen afvigelser konstateret.
11.1.2 Fysisk adgangskontrol ▶ Alene autoriserede personer har adgang til datacenteret via den etablerede procedure. ▶ Eksterne personers (leverandører eller kunder) adgang til lokalet, sker i følgeskab med en autoriseret medarbejder.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politik for tildeling af rettigheder til personale og leverandører, og vi har observeret, at adgange til datacentret tildeles efter roller og ansvar i organisationen. Vi har inspicereret log over adgange til datacentret hos Sentia A/S og observeret, at der er tildelt adgang i overensstemmelse med arbejdsbetinget behov og at eksterne personer følges af en autoriseret medarbejder.	Ingen afvigelser konstateret.
11.1.3 Sikring af kontorer, lokaler og faciliteter ▶ Serviceleverandørens kontorlokaler er monteret med tyverialarm. ▶ Kun personer med et arbejdsbetinget behov, tildeles adgang til serviceleverandørens kontor.	Vi har udført forespørgsler hos relevant personale. Vi har foretaget fysisk inspektion af kontorlokaler og observeret, at der er installeret tyverialarm med bevægelsesfølere i kontorlokalerne.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

Kontrolmål 11.1 – Sikre områder

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspicereret tildelte adgange til kontoret og observeret, at det er givet i overensstemmelse med et arbejdsbetinget behov.	

A.12 Driftssikkerhed

Kontrolmål 12.1 – Driftsprocedurer og ansvarsområder

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
12.1.2 Ændringsstyring ▶ Serviceleverandøren har defineret en proces for ændringshåndtering for at sikre, at ændringer sker efter aftale med kunder og er tilrettelagt hensigtsmæssigt i forhold til interne forhold. ▶ Større ændringer sker alene baseret på en klassificering af opgaven, kompleksiteten og vurdering af påvirkning af andre systemer.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for ændringer i driftsplatform og applikationer og observeret, at denne anfører, at der bland andet skal udføres en risikovurdering og plan for ændringen. Vi har for en stikprøve af ændringer i erklæringsperioden observeret, at ændringerne er testet inden frigivelse.	Ingen afvigelser konstateret.
12.1.3 Kapacitetsstyring ▶ Serviceleverandøren har via overvågningssystem opsat grænseværdier for, hvornår overordnede systemer og dermed kunders systemer skal skaleres op af hensyn til elektronisk plads, svar tider mv. ▶ Når serviceleverandøren opsætter nye systemer, foretages test af funktionalitet, herunder kapacitet-og performancetest.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret grænseværdierne i overvågningssystemet, og vi har observeret, at alarm aktiveres, såfremt servernes kapacitet overstiger de tilladte værdier. Vi har inspiceret dokumentation for den udførte kapacitets overvågning er foretaget i henhold til politikken for kapacitetsstyring. Vi har ved forespørgsel fået oplyst, at ingen nye systemer blev opsat i erklæringsperioden, hvorfor vi ikke har kunne verificere, hvorvidt der har været foretaget test af funktionalitet, kapacitet- og performancetest.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

Kontrolmål 12.2 – Beskyttelse mod malware

- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
12.2.1 Kontroller mod malware • Serviceleverandøren har implementeret scannings- og overvågningssystemer til at sikre mod kendt skadevoldende kode. • Serviceleverandøren har antivirus-systemer, systemer til overvågning af internetbrug, trafik og ressourcer på RDP-platforme samt sikringer i øvrige tekniske og centrale installationer (firewall mv.).	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret oversigten over firewall og observeret, at firewallen var aktiveret. Vi har observeret overvågning af antivirus for udvalgte kunders server, og vi har observeret, at der foretages scanninger af enhederne. Vi har inspicereret AV-konsollen og observeret, at AV-signaturer er opdateret på alle relevante enheder. Vi har inspicereret oversigten over firewall for udvalgte kunder, og vi har observeret, at der er tekniske installationer, som sikrer netværket.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

Kontrolmål 12.3 - Sikkerhedskopiering

- *At beskytte mod tab af data.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
12.3.1 Sikkerhedskopiering af information ▶ Serviceleverandøren sikrer at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis samt efter de aftaler, som serviceleverandøren har med kunder. ▶ Serviceleverandøren har etableret en testplan for verificering af, hvorvidt sikkerhedskopieringen fungerer, samt en test af, hvordan systemer og data praktisk kan reetableres. ▶ Medmindre andet er aftalt med kunder, foretager serviceleverandøren sikkerhedskopiering af hele deres virtuelle miljø.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politikker og procedurer, og vi har observeret, at sikkerhedskopieringen udføres dagligt for kunderne, medmindre andet er aftalt. Vi har stikprøvevis udvalgt en kunde og observeret, at der er udført sikkerhedskopiering dagligt. Vi har inspiceret en udvalgt kunde og observeret, at data er blevet genskabt efter kundens ønske.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

Kontrolmål 12.4 - Logning og overvågning

- *At registrere hændelser og tilvejebringe bevis.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
12.4.1 Hændelseslogning - Serviceleverandøren har et overvågningssystem, hvor driftskritiske servere og udstyr overvåges. - Serviceleverandøren opsamler logs for alle servere og enheder i netværket.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret overvågningssystemet og observeret, at kritiske servere og udstyr overvåges. Vi har inspicereret overvågning for udvalgt server og observeret, at der var opsat logning i erklæringsperioden.	Ingen afvigelser konstateret.
12.4.2 Beskyttelse af logoplysninger - Serviceleverandøren beskytter log-oplysninger mod manipulation og uautoriserede adgang på 2 af hinanden uafhængige lagersystemer.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret to systemer, hvorpå loggen opsamles, og vi har observeret, at oplysningerne bliver beskyttet.	Ingen afvigelser konstateret.
12.4.3 Administrator- og operatørlog - Serviceleverandøren opsamler log fra udstyr som vedrører driften.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret log over administratorer og operatører i Windows og for en stikprøve observeret, at alle hændelser foretaget af disse, logges.	Ingen afvigelser konstateret.
12.4.4 Tidssynkronisering - Serviceleverandøren har sikret, at urene i informationsbehandlingssystemer er synkroniseret og har samme tidsstempel.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret tidssynkroniseringen for udvalgte enheder, og observeret, at tidssynkronisering er slået til.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

Kontrolmål 12.6 - Sårbarhedsstyring

- *At forhindre, at tekniske sårbarheder udnyttes.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
12.6.1 Styring af tekniske sårbarheder ▶ Serviceleverandøren indsamler information og aktuelle sårbarheder via DK Cert og leverandører.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret tickets for stillingtagelse til e-mails, modtaget fra Microsoft og DK Cert, og har for en stikprøve af mails fra DK Cert observeret, at der er taget stilling til disse.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

Kontrolmål 13.1 - Styring af netværkssikkerhed

- *At sikre beskyttelse af information i netværk og af understøttende informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
13.1.1 Netværksstyring ▶ Adgang til serviceleverandørens netværksudstyr er tildelt efter rolle og arbejdsopgaver for medarbejdere. ▶ Adgang til de enkelte netværksenheder og netværkstjenester er etableret med værktøjet til remote access. Værktøjet styrer brugeradgang og passwords. ▶ Intern adgang til netværksudstyr kan kun etableres gennem en krypteret remote desktop (RDP) forbindelse med to-faktor godkendelse. ▶ Der er indlagt kontroller for adgangsrettigheder til netværksudstyr og netværkstjenester.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret oversigt over firewall og observeret, at kun godkendt medarbejdere kan tilgå netværksudstyr. Vi har inspiceret kundernes netværk og observeret, at der er funktionsadskillelse. Vi har inspiceret adgange til netværksudstyr og observeret, at adgang sker med en to-faktor godkendelse. Vi har inspiceret dokumentation for at gennemgang af brugeradgange er foretaget og observeret, at der er udført kvartalsvis kontrol af ansattes adgangsrettigheder til netværksudstyr og netværkstjenester.	Ingen afvigelser konstateret.
13.1.2 Sikring af netværkstjenester ▶ Alene godkendt netværkstrafik (indgående) kommer gennem serviceleverandørens firewall.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret systemkonfiguration for switch og firewall, og observeret, at netværkstrafik er beskyttet af firewall.	Ingen afvigelser konstateret.
13.1.3 Opdeling af netværk ▶ Serviceleverandørens netværk er opdelt på forskellige VLAN (Virtual Local Area Network) for at sikre separation mellem kunderne.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret systemkonfiguration for netværk og observeret, at kundenetværk er adskilt på separate VLAN.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

Kontrolmål 13.2 - Informationsoverførsel

- *At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
13.2.1 Politikker og procedurer for informationsoverførsel ▶ Fortrolige informationer, der udveksles via e-mails, skal sikres i overensstemmelse med serviceleverandørens informationer, der er klassificeret i henhold til politikken, angivet i dokumentet om klassifikation af information og aktiver. ▶ Kodeord til kundesystemer må alene fremsendes som angivet i dokumentet om procedure for systemadgang for hosting-kunder. ▶ Glemte kodeord håndteres via procedure, som er angivet i dokumentet om procedure for identifikation af brugere ved udlevering af nyt password til sikring af, at kun godkendte personer kan få udstedt og oplyst et nyt password.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret politik for informationsoverførsel og observeret, at politikken definerer retningslinjer for kommunikation. Vi har observeret, at TLS 1.2 er opsat på mailserveren. Vi har ved forespørgsel fået oplyst, at ingen fortrolige informationer er blevet sendt via e-mail i erklæringsperioden, hvorfor vi ikke har kunne verificere effektiviteten af denne del af politikken. Vi har ved interview med relevante medarbejdere fået bekræftet medarbejdernes forståelse for kommunikationssikkerhed og informationsoverførsel. Vi har for en stikprøve inspiceret kommunikation af password til bruger og observeret, at procedure for informationsoverførsel af fortrolig karakter bliver fulgt.	Ingen afvigelser konstateret.
13.2.2 Aftaler om informationsoverførsel ▶ Serviceleverandøren har indgået aftaler om informationsoverførsel med kunder og leverandører, som skal sikre, at lovgivning overholdes, og at samarbejdet er formaliseret.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik for aftaler om informationsoverførsel mellem serviceleverandøren og eksterne parter og observeret, at det fremgår heraf at informationsoverførsel aftales via kontrakten, når en aftale indgås med en kunde. Vi har ved forespørgsel fået oplyst, at der ikke er indgået aftaler om informationsoverførsel i erklæringsperioden. Vi har inspiceret dokumentation på at en aftale om informationsoverførsel foreligger hos en stikprøvevis udvalgt eksisterende kunde.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

Kontrolmål 13.2 - Informationsoverførsel

- *At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
13.2.3 Elektroniske meddelelser ▶ Ekstern datakommunikation sker alene via e-mails, idet kunders adgang og brug af servere ikke betragtes som ekstern datakommunikation.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret udvalgt korrespondance med kunde og observeret, at det er foretaget ved brug af e-mail. Vi har inspicereret kryptering og observeret, at serviceleverandøren anvender TLS kryptering.	Ingen afvigelser konstateret.
13.2.4 Fortroligheds- og hemmeligholdelsesaftaler ▶ Serviceleverandørens fortroligheds- og hemmeligholdelsesaftale (Non Disclosure Agreement – NDA) benyttes til kunder såvel som kontrahenter.	Vi har udført forespørgsler hos relevant personale. Vi har ved forespørgsel fået oplyst, at der ikke er indgået nye databehandleraftaler i erklæringsperioden. Vi har inspiceret dokumentation på at en fortroligheds- og hemmelighedsaftale foreligger hos en stikprøvevis udvalgt eksisterende kunde.	Ingen afvigelser konstateret.

A.14 Anskaffelse, udvikling og vedligeholdelse af systemer

Kontrolmål

- *At sikre, at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
14.1.1 Analyse og specifikation af informationssikkerhedskrav ▶ Der er implementeret procedurer for stillingtagelse til passende informationssikkerhedsmæssige krav	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret procedure for analyse og stillingtagen til informationssikkerhedsmæssige krav i forbindelse med anskaffelse, udvikling og vedligeholdelse af systemer. Vi har ved forespørgsel fået oplyst, at ingen nye systemer er blevet implementeret i erklæringsperioden, hvorfor vi ikke har kunne verificere, at der er taget passende stilling til informationssikkerhedsmæssige krav i erklæringsperioden.	Ingen afvigelser konstateret
14.1.2 Sikring af applikationstjenester på offentlige netværk ▶ Der er taget stilling til hvordan informationer der transporteres gennem offentlige netværker beskyttes mod svindel, kontraktlige uoverensstemmelser og uautoriseret offentliggørelse og ændring.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at der føres kontrol med SSL-certifikater og Nessus scanninger og stikprøvevis påset disse.	Ingen afvigelser konstateret

A.15 Leverandørforhold

Kontrolmål 15.1 - Informationssikkerhed i leverandørforhold

- *At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
15.1.1 - Informationssikkerhedspolitik for leverandørforhold ▶ Det kræves, at leverandørernes informationssikkerhedsniveau lever op til kravene i serviceleverandørens informationssikkerhedspolitik for leverandører. Dette sikres gennem kontrakter, NDA eller databehandleraftale.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret informationssikkerhedspolitik for leverandører. Vi har ved forespørgsel fået oplyst, at informationssikkerhedspolitikken sendes til leverandører, når en aftale indgås. Vi har for en stikprøve af nye leverandører inspiceret dokumentation for, at underleverandøren er blevet introduceret til serviceleverandørens informationssikkerhedspolitik for leverandører, og vi er ved forespørgsel blevet informeret om, at de accepterede den.	Ingen afvigelser konstateret.
15.1.2 - Håndtering af sikkerhed i samarbejdspartnere og leverandøraftaler ▶ Underleverandører har kvitteret for at have læst og forstået serviceleverandørens sikkerhedspolitik for leverandører samarbejde.	Vi har udført forespørgsler hos relevant personale. Vi har for en stikprøve af nye leverandører inspiceret dokumentation for, at underleverandøren er blevet introduceret til serviceleverandørens informationssikkerhedspolitik for leverandører, og vi er ved forespørgsel blevet informeret om, at de accepterede den.	Ingen afvigelser konstateret
15.2.1 - Overvågning og gennemgang af samarbejdspartnere og leverandørydelser ▶ Serviceleverandøren udfører regelmæssig overvågning af sine samarbejdspartnere ved at indhente relevante materiale der understøtter deres efterlevelse af aftalte forpligtelser.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret, at der ført tilsyn af underleverandørers erklæringer ISAE 3402 erklæringer og at der er taget stilling til deres indehold og at ingen afvigelser er blevet identificeret hvorfor ingen yderligere handlinger er fundet nødvendige	Ingen afvigelser konstateret.

A.15 Leverandørforhold

Kontrolmål 15.1 - Informationssikkerhed i leverandørforhold

- *At sikre beskyttelse af organisationens aktiver, som leverandører har adgang til.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
15.2.2 - Styring af ændringer af samarbejdspartnere og leverandørydelser ▶ Serviceleverandøren har procedurer for at kontrollere ændringer i driften i forbindelse med ændringer i indgåede aftaler med samarbejdspartnere og leverandører.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret relevante procedurer og observeret, at der skal føres kontrol af samarbejdspartneres ydelser. Vi har ved forespørgsel fået oplyst, at dette er gjort og at ingen ændringer er foretaget i driften i erklæringsperioden.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

Kontrolmål 16.1 - Styring af informationssikkerhed og forbedringer

- *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
16.1.1 Ansvar og procedurer ▶ Serviceleverandøren har procedurer for håndtering af hændelser, såsom opdateringer af patches, virusinficerede filer og systemer, overvågning for hackerangreb mv. for at sikre beskyttelse af kunders systemer og data.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedurer for håndtering af sikkerhedshændelser og observeret, at ledelsen har godkendte procedurer og politikker for håndtering af sikkerhedshændelser.	Ingen afvigelser konstateret.
16.1.2 Rapportering af informationssikkerhedsbrud ▶ Medarbejdere og eksterne samarbejdspartnere er, via de indgåede kontrakter og aftaler, forpligtet til at anmeldelse enhver sikkerhedshændelse til nærmeste leder, så der hurtigst muligt kan reageres på hændelsen, og nødvendige tiltag kan udføres.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret skabelon for rapporteringsskema og observeret, at medarbejdere skal registrere og rapportere sikkerhændelser, der måtte forekomme. Vi har ved forespørgsel blevet informeret om, at der ikke har været informationssikkerhedsbrud i erklæringsperioden, hvorfor vi ikke kunne verificeret effektiviteten af proceduren.	Ingen afvigelser konstateret.
16.1.3 Rapportering af informationssikkerhedssvagheder ▶ Til styring af overvågning og opfølgning på hændelser har serviceleverandøren implementeret formelle incident- og problem management procedurer, der sikrer, at hændelser registreres, prioriteres, styres, eskaleres, og at der foretages de nødvendige handlinger. Forløbet dokumenteres i ticket systemet.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedurer for håndtering af incident og problem management og observeret, at der heri er processer for håndtering af informationssikkerhedsbrud. Vi har inspiceret dokumentation for informationssikkerhedshændelser i erklæringsperioden er dokumenteret i ticket-systemet i henhold til proceduren.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

Kontrolmål 16.1 – Styring af informationssikkerhed og forbedringer

- *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
16.1.4 Vurdering af og beslutning om informationssikkerhedshændelser ▶ Sikkerhedshændelser afstedkommet fra hhv. egne observationer, alarmering ud fra log- og overvågningssystem, telefoniske henvendelser fra kunder, underleverandører eller samarbejdspartnere, blive eskaleret til teknisk afdeling med samtidig orientering til ledelsen.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret procedurer for styring og opfølgning på hændelser og observeret, at der heri er anført at informationssikkerhedshændelser skal vurderes. Vi har inspiceret at den indtrådte informationssikkerhedshændelse er blevet behandlet i overensstemmelse med serviceleverandørens relevante procedure, og at den ikke blev registreret som et informationssikkerhedsbrud da hændelsen blev stoppet før det blev til et brud.	Ingen afvigelser konstateret.
16.1.5 Håndtering af informationssikkerhedsbrud ▶ Sker en hændelse inden for normal arbejdstid, vil serviceleverandøren håndtere og eskalere sagen på samme vis som andre sager og med den prioritering, som er nødvendig.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for håndtering af informationssikkerhedsbrud og observeret, at der skal udfyldes en hændelsesrapport. Vi har inspicereret hændelsesrapporten og observeret, at kunderne skal kontaktes og forløbet dokumenteres i ticket-systemet. Vi har ved forespørgsel blevet informeret om, at der ikke har været informationssikkerhedsbrud i erklæringsperioden, hvorfor vi ikke har verificeret effektiviteten af proceduren.	Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

Kontrolmål 16.1 – Styring af informationssikkerhed og forbedringer

- *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
16.1.6 Erfaring fra informationssikkerhedsbrud ▶ Serviceleverandørens logføring og øvrige overvågningssystemer vil kunne benyttes til at evaluere på sikkerhedshændelsen.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret skabelon for informationssikkerhedshændelser og svagheder og observeret, at medarbejderne skal notere de erfaringer, som de har fået. Vi er ved forespørgsel blevet informeret om, at der ikke har været informationssikkerhedsbrud i erklæringsperioden, men vi har observeret at proceduren efterleves idet der er taget erfaring af indtrådte informationssikkerhedshændelser. Vi har inspiceret dokumentation for informationssikkerhedshændelse i erklæringsperioden og observeret, at erfaringsopsamling er foretaget i hændelsesrapporten.	Ingen afvigelser konstateret.
16.1.7 Indsamling af beviser ▶ Serviceleverandøren foretager en root cause analyse for at sikre, at de opståede sikkerhedshændelser ikke gentager sig.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret skabelon for hændelsesrapport, og vi har observeret, at årsagerne til sikkerhedsbruddet opsamles i en log. Vi har inspiceret dokumentation for at der er samlet beviser for indtrådte hændelser og observeret, at relevant dokumentation er blevet indhentet.	Ingen afvigelser konstateret.

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

Kontrolmål 17.1 - Informationssikkerhedskontinuitet

- *Informationssikkerhedskontinuiteten skal være forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
17.1.1 Planlægning af informationssikkerhedskontinuitet ▶ Serviceleverandøren har udarbejdet en overordnet beredskabsplan.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret politik og procedurer for beredskabsplan og observeret, at der er etableret en beredskabsplan til håndtering af nedbrud.	Ingen afvigelser konstateret.
17.1.2 Implementering af informationssikkerhedskontinuitet ▶ Serviceleverandørens beredskabsplan er forankret i it-risikoanalysen og vedligeholdes minimum årligt i forlængelse af udførelsen af analysen.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for beredskabsplanen og observeret, at beredskabsplanen er udarbejdet på baggrund af den udførte it-risikoanalyse. Vi har inspiceret dokumentation for at beredskabsplanen er blevet gennemgået i erklæringsperioden.	Ingen afvigelser konstateret.
17.1.3 Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten ▶ Serviceleverandøren tester beredskabsplanen en gang årligt som en del af det overordnede beredskab.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret dokumentation for test af beredskabsplanen i erklæringsperioden og observeret, at ledelsen har gennemgået og foretaget en vurdering af den udførte test.	Ingen afvigelser konstateret.

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

Kontrolmål 17.2 – Redundans

- *At sikre tilgængelighed af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
17.2.1 Tilgængelighed af informantionsbehandlingsfaciliteter ▶ Planen og procedurerne er forankret i serviceleverandørens driftsdokumentation og procedurer.	Vi har udført forespørgsler hos relevant personale. Vi har inspicereret proceduren for beredskabsplan og observeret, at medarbejderne har adgang til proceduren og planen.	Ingen afvigelser konstateret.

A.18 Overensstemmelse

Kontrolmål 18.1 - Overensstemmelse med lov- og kontraktkrav

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
18.1.1. Identifikation af gældende lovgivning og kontraktkrav ▶ Serviceleverandøren er ikke underlagt særlig lovgivning i forhold til ydelserne. Serviceleverandørens kunder kan dog være, og for de steder er understøttelse heraf aftalt særskilt.	Vi har udført forespørgsler hos relevant personale. Vi har ved forespørgsel blevet informeret om, at der ikke er indgået nye kundekontrakter i erklæringsperioden, hvorfor vi ikke har kunne verificere, hvorvidt der i forbindelse med nye kunder er blevet kontrolleret at særlovgivning skal følges.	Ingen afvigelser konstateret.
18.1.3. Beskyttelse af registreringer ▶ Serviceleverandørens fører regelmæssig kontrol af at hosting data er tilstrækkelig teknisk beskyttet imod udefrakommende trusler og menneskelige fejl.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret dokumentation for at serviceleverandøren har ført regelmæssig kontrol af at hosting data er tilstrækkelig beskyttet mod udefrakommende trusler og menneskelige fejl.	Ingen afvigelser konstateret.
18.2.1 Uafhængig gennemgang af informationssikkerhed ▶ Serviceleverandøren lader årligt revideres af ekstern revisor med henblik på afgivelse af erklæring for overholdelsen af kontrollerne, nævnt i denne beskrivelse.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret serviceleverandørens politik for gennemgang af informationssikkerheden og observeret, at der årligt skal udarbejdes en ISAE 3402 erklæring fra uafhængig revisor. Vi har udarbejdet nærværende ISAE 3402-erklæring til brug for serviceleverandørens forpligtelser i denne relation.	Ingen afvigelser konstateret.
18.2.2 Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder ▶ Serviceleverandøren har en intern kontrol, der undersøger, om de etablerede politikker og retningslinjer overholdes af medarbejderne.	Vi har udført forespørgsler hos relevant personale. Vi har inspiceret procedurer for gennemgang af sikkerhedspolitikker og sikkerhedsstandarder og observeret, at der heri fremgår at ledelsen skal sikre, at medarbejdere er bekendt med serviceleverandørens informationssikkerhedspolitik.	Ingen afvigelser konstateret.

A.18 Overensstemmelse

Kontrolmål 18.1 – Overensstemmelse med lov- og kontraktkrav

- *At forhindre overtrædelse af lov-, myndigheds- eller kontraktkrav i relation til informationssikkerhed og andre sikkerhedskrav.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har inspiceret dokumentation for at serviceleverandøren har ført regelmæssig kontrol af at politikker og retningslinjer er overholdt.	

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB

KYSTVEJEN 29
8000 AARHUS C

CVR-NR. 20 22 26 70