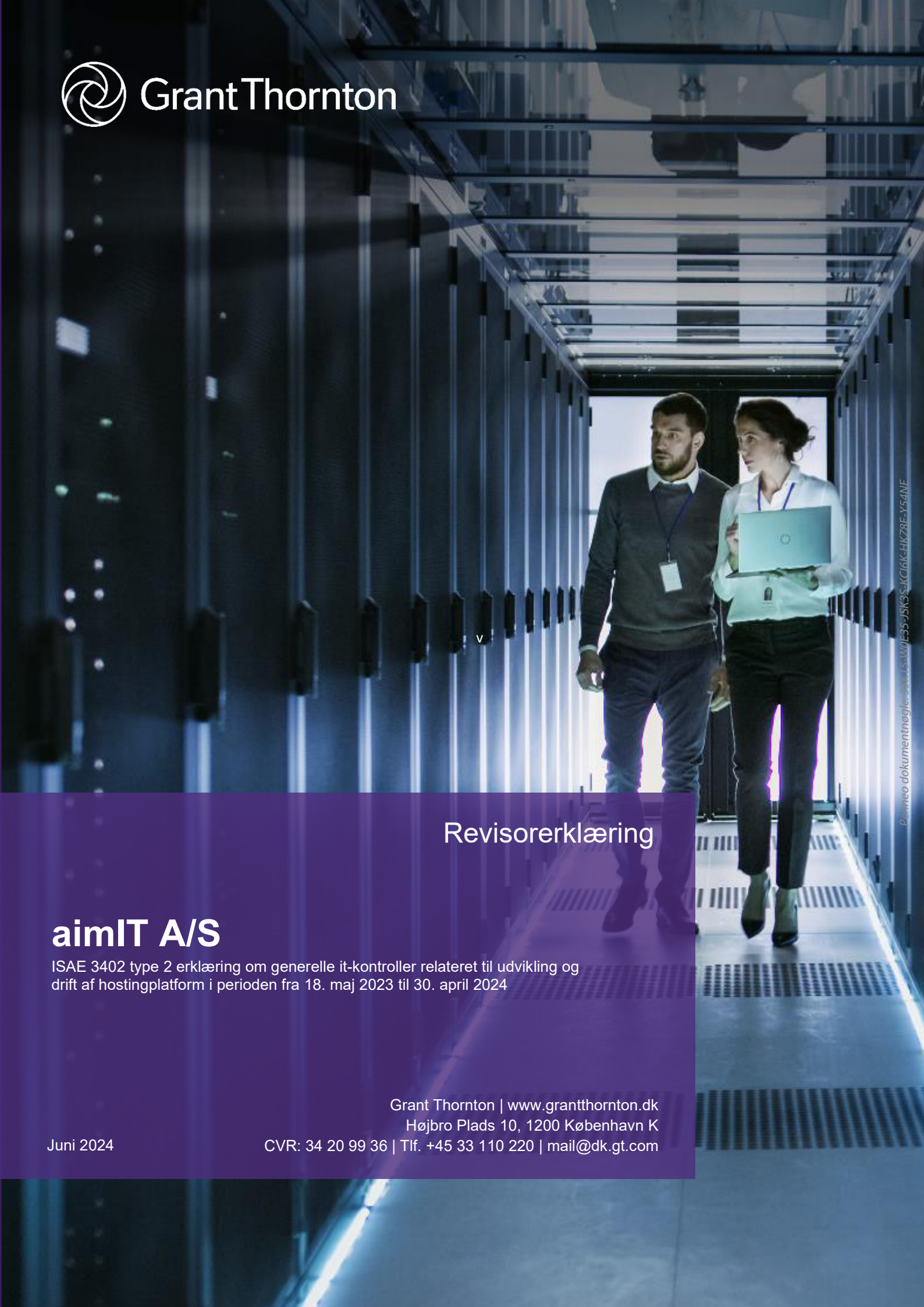

Revisorerklæring

aimIT A/S

ISAE 3402 type 2 erklæring om generelle it-kontroller relateret til udvikling og drift af hostingplatform i perioden fra 18. maj 2023 til 30. april 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Juni 2024

Indholdsfortegnelse

Sektion 1: aimIT A/S' udtalelse

Medfølgende beskrivelse er udarbejdet til brug for kunder, der har anvendt aimIT A/S' udvikling og drift af hostingplatform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne selv har anvendt, ved vurdering af risiciene for væsentlig fejlinformation i kundernes regnskaber.

aimIT A/S anvender underleverandørerne Curanet A/S og GlobalConnect. Denne erklæring er udarbejdet efter partielmetoden, og aimIT A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Curanet A/S og GlobalConnect. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af vores kontroller, er passende designet og er operationelt effektive. Beskrivelsen omfatter ikke kontrolaktiviteter udført af underleverandører.

aimIT A/S bekræfter, at:

(a) Den medfølgende beskrivelse i Sektion 3, giver en retvisende beskrivelse af de generelle it-kontroller med relevans for aimIT A/S' udvikling og drift af hostingplatform der har behandlet kunders transaktioner i perioden fra 18. maj 2023 til 30. april 2024. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

   (i) Redegør for, hvordan kontrollerne har været designet og implementeret, herunder redegør for:

   - De typer af ydelser, der er leveret.
   - De processer i både it- og manuelle systemer, der er anvendt til styring af de generelle it-kontroller.
   - Relevante kontrolmål og kontroller designet til at nå disse mål.
   - Kontroller, som vi med henvisning til kontrollernes design har forudsat ville være implementerede af brugervirksomheder, 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 og kommunikation, kontrolaktiviteter og overvågningskontroller, som har været relevante for de generelle it-kontroller.

   (ii) Indeholder relevante oplysninger om ændringer i de generelle it-kontroller foretaget i perioden fra 18. maj 2023 til 30. april 2024.

   (iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af det beskrevne system under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved systemet, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt designet og operationelt effektive i perioden fra 18. maj 2023 til 30. april 2024, hvis relevante kontroller hos underleverandører var operationelt effektive, som forudsættes i designet af aimIT A/S' kontroller i hele perioden fra 18. maj 2023 til 30. april 2024. Kriterierne for denne udtalelse var, at:

   (i) De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret

   (ii) De identificerede kontroller ville, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål, og

   (iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetencer og beføjelser i perioden fra 18. maj 2023 til 30. april 2024.

Birkerød, den 26. juni 2024
aimIT A/S

Carsten Alnøe
Adm. direktør

Sektion 2: Uafhængig revisors erklæring om beskrivelsen af kontroller, deres design og operationelle effektivitet

Til aimIT A/S, deres kunder, og deres revisorer.

Omfang

Vi har fået som opgave at afgive erklæring om aimIT A/S' beskrivelse i Sektion 3 af generelle it-kontroller for drift af brugersystemer til behandling af aimIT A/S' udvikling og drift af hostingplatform i perioden og om design og operationel effektivitet af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

aimIT A/S anvender underleverandørerne Curanet A/S og GlobalConnect. Denne erklæring er udarbejdet efter partielmetoden, og aimIT A/S' kontrolbeskrivelse omfatter ikke kontrolmål og tilknyttede kontroller hos Curanet A/S og GlobalConnect. Visse kontrolmål i beskrivelsen kan kun nås, hvis underleverandørernes kontroller, der forudsættes i designet af aimIT A/S´ kontroller, er passende designet og operationelt effektive sammen med de relaterede kontroller hos aimIT A/S.

aimIT A/S' ansvar

aimIT A/S er ansvarlig for udarbejdelsen af beskrivelsen i Sektion 3 og tilhørende udtalelse i Sektion 1, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udtalelsen er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for designet og implementeringen af operationelt effektive kontroller for at nå de anførte kontrolmål.

Grant Thorntons 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.

Grant Thornton anvender International Standard on Quality Management 1, ISQM 1, som kræver, at vi designer, implementerer og driver et kvalitetsstyringssystem, herunder politikker eller procedurer vedrørende overholdelse af etiske krav, faglige standarder og gældende lov og øvrig regulering.

Revisors ansvar

Vores ansvar er på grundlag af vores handlinger at udtrykke en konklusion om aimIT A/S' beskrivelse (Sektion 3) og om designet og den operationelle effektivitet af kontroller, der knytter sig til de kontrolmål, der er anført i denne beskrivelse.

Vi har udført vores arbejde i overensstemmelse med ISAE 3402, "Erklæringer med sikkerhed om kontroller hos en serviceleverandør", som er udstedt af IAASB og yderligere krav ifølge dansk revisorlovgivning.

Denne standard kræver, at vi planlægger og udfører vores handlinger for at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er retvisende, og at kontrollerne i alle væsentlige henseender er hensigtsmæssigt designet og operationelt effektive.

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen, designet og den operationelle effektivitet af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system og for kontrollernes design 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 designet eller ikke er operationelt effektive. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået.

En erklæringsopgave med sikkerhed af denne type omfatter desuden en vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som serviceleverandøren har specificeret og beskrevet aimIT A/S' udtalelse i Sektion 1.

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

aimIT A/S' beskrivelse i Sektion 3 er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter ved de generelle it-kontroller, 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 afdække alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten 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 aimIT A/S' udtalelse i Sektion 1. Det er vores opfattelse, at:

(a) Beskrivelsen af de generelle it-kontroller, således som de var designet og implementeret i perioden 18. maj 2023 til 30. april 2024, i alle væsentlige henseender er retvisende
(b) Kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt designet i perioden fra 18. maj 2023 til 30. april 2024, for at give høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, ville blive opnået, hvis kontroller hos underleverandører var operationelt effektive, der forudsættes i designet af aimIT A/S' kontroller i perioden fra 18. maj 2023 til 30. april 2024
(c) De testede kontroller, som var de kontroller, der var nødvendige for at give en høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har været operationelt effektive i perioden 18. maj 2023 til 30. april 2024

Beskrivelse af test af kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår i den efterfølgende Sektion 4 om kontrolmål, udførte kontroller, test og resultater heraf.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller i Sektion 4 er udelukkende tiltænkt kunder, der har anvendt aimIT A/S' udvikling og drift af hostingplatform, og deres revisorer, som har en tilstrækkelig forståelse til at overveje den sammen med anden information, herunder information om kunders egne kontroller, når de vurderer risiciene for væsentlige fejlinformationer i deres regnskaber.

København, den 26. juni 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Anders Holmgaard Christiansen
Statsautoriseret revisor

Isabella Ørgaard Jensen
Director, CISA

Sektion 3: Beskrivelse af aimIT A/S' ydelser i forbindelse med udvikling og drift af hostingplatform samt generelle it-kontroller relateret hertil

aimIT A/S er et it-løsningshus etableret i 1998 og har siden 2019 haft hovedkontor i Birkerød, hvorfra vi fokuserer på at levere it-drift og -service med kunderne i centrum. aimIT tilbyder konsulentydelser på flere niveauer, og kan bruges til ad hoc-opgaver, som trusted advisor eller som virksomhedens outsourcede it-afdeling. Kunderne er både små og mellemstore virksomheder inden for den private og offentlige sektor.

aimIT leverer it-løsninger fra udvalgte producenter og udover at understøtte kundernes daglige it -indkøb er der særlig fokus på brugersupport, sikkerhedsprodukter, server/storage, backup, Wi-Fi løsninger, Firewall løsninger og i særdeleshed Hosting.

aimIT har stor fokus på GDPR og har derfor to Tier3 datacentre på eksterne adresser i Danmark. Med fokus på compliance har datacentrene ISAE-3402 type 2 samt ISAE-3000 erklæringer.

Målsætningen er at skabe merværdi for kunderne i den daglige it-drift, samt have langvarige seriøse kunderelationer, yde en professionel og god kundeservice og sikre stabil drift og/eller den bedste oppetid/dækning til vores kunder.

Generelle IT-kontroller hos aimIT

Indledning
I det følgende beskrives de generelle it-kontroller relateret til aimIT's ydelser til kunder jf. beskrivelsen ovenfor i Sektion 1.

Risikostyring

Med udgangspunkt i risikovurderingen og ISO 27001/2:2013 har aimIT udvalgt hovedområder og kontrolmål for styring af it-sikkerheden. Risikovurdering afdækker risici forbundet med drift såvel som risici tilknyttet brug af diverse underleverandører. Ligeledes, er der i risikovurderingen taget højde for mitigerende tiltag ved de identificerede risici. Risikovurderingen bliver gennemgået minimum årligt af ledelsen.

Organisering af IT-sikkerheden

Organiseringen af IT-sikkerheden sker med udgangspunkt i aimIT's it-sikkerhedspolitik og tager udgangspunkt i ISO 27001/2:2013, som indeholder følgende hovedområder:

5	Informationssikkerhedspolitikker	12	Driftssikkerhed
6	Organisering af informationssikkerhed	13	Kommunikationssikkerhed
8	Styring af aktiver	15	Leverandørforhold
9	Adgangsstyring	16	Styring af informationssikkerhedsbrud.
10	Kryptografi	17	Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
11	Fysisk sikring og miljøsikring	18	Overensstemmelse

Tilrettelæggelsen af IT-sikkerheden indenfor de enkelte områder er beskrevet nedenfor. Kontrolmål og kontroller som aimIT har udvalgt, fremgår desuden af oversigten i Sektion 4.

Informationssikkerhedspolitikker

aimIT har en informationssikkerhedspolitik der afdækker diverse områder inden for styring af informationssikkerheden. Politikken er gjort tilgængelig for samtlige medarbejdere. Det er påkrævet, at aimIT's medarbejdere har læst og er indforstået med politikken. Ledelsen sikrer, at politikken bliver gennemgået og hvis påkrævet opdateret minimum årligt.

Intern organisering

aimIT har klart definerede roller og ansvarsområder for informationssikkerheden. Disse roller er defineret i informationssikkerhedspolitikken såvel som i ét organisationsdiagram. På denne måde sikres det, at der er funktionsadskillelse og alle medarbejdere i aimIT har en klar idé om deres ansvar i relation til informationssikkerhed.

aimIT har i forbindelse med vores drift løbende kontakt til Danish Cloud Community, hvor vi er medlem. Vi bliver løbende informeret om relevante ændringer i lovgivningen, herunder GDPR.

Mobilt udstyr og fjernarbejdspladser

aimIT har udarbejdet en politik, som udstikker retningslinjer for anvendelsen af mobile enheder og hjemmearbejdspladser, som aimIT's medarbejdere har læst og er forpligtet til at følge. Hjemmearbejdspladser er sikret via krypteret VPN-forbindelse med 2 faktor godkendelse.

Medarbejdersikkerhed

Generelle vilkår for ansættelse, herunder både fortrolighed om firmaets egne og kundernes forhold samt roller og ansvar, er beskrevet i hver medarbejders ansættelseskontrakt samt i personalehåndbogen. Dokumenterne er underskrevet ved kontraktindgåelse med den enkelte medarbejder af både ledelsen og medarbejderen.

Ansættelsesforholdets ophør eller ændring
Der er opsat formaliserede processor for når en medarbejder stopper. Ved fratrædelse lukkes alle adgange inden den ansatte forlader kontoret. Alle udleverede enheder skal efterlades med dokumenteret koder. Det overordnede ansvar for sikring af alle kontroller i fratrædelsesprocessen ligger hos aimIT's ledelse.

Styring af aktiver
Informationssikkerhedspolitikken omfatter alle aktiver, som understøtter aimIT's forretningsområder og organisation. Disse omfatter data, systemer, fysiske aktiver samt tekniske forsyninger, der understøtter IT anvendelsen. Der er tilskrevet politikker for styring af aktiver som er tilgængeliggjort for aimIT's medarbejdere.

Ansvar for aktiver
aimIT's aktiviteter er registreret og opmærket i en fortegnelse over aktiver. Dette giver bl.a. overblik over, hvor aktivet befinder sig, hvem der bruger det, hvornår og hvor det er købt samt hvilket serienummer og garanti, der er på aktivet. I forlængelse af dette, har aimIT klart definerede retningslinjer for brug og håndtering af aktiver. Disse retningslinjer er kommunikeret ud til medarbejderne i personalehåndbogen sammen med vores informationssikkerhedspolitik.

Mediehåndtering

aimIT har definerede retningslinjer for mediehåndtering og ligeledes for bortskaffelse af medier. Der er lukket af for brug af USB-nøgler og flytbare medier. Alt databærende udstyr formateres og fabriksnulstilles inden bortskaffelse via Dansk Sikkerheds Makulering.

Adgangsstyring

Adgangsstyring stiller krav til sikring af adgang til systemer og data. Systemer og data, herunder teknisk basisprogrammel, er sikret mod uberettiget eller utilsigtet adgang. Tildelingen af adgangsrettigheder m.v. sker ud fra et arbejdsbetinget behov og under hensyntagen til en effektiv funktionsadskillelse.

Ved nyansættelse oprettes der en medarbejderprofil med præcis de adgangsmuligheder, som skal til for at kunne løse de opgaver, medarbejderen ansættes til. Ændres en medarbejders opgaver, ændrer sikkerhedschefen adgangsmulighederne tilsvarende.

It-sikkerhedspolitikken beskriver at vores medarbejderes kodeord er personlige, og det er alene brugeren selv, der må kende kodeordet. Medarbejdere skal årligt skrive under på, at de har læst og forstået seneste version af vores it-sikkerhedspolitik. I forlængelse af dette, sikrer aimIT løbende, at medarbejderne har de korrekte arbejdsbetingede adgangsrettigheder. Dette bliver gjort via en formaliseret gennemgang af adgangsrettighederne i de diverse systemer der anvendes i aimIT.

Kryptografi

Kryptografiske kontroller
Kryptering skal anvendes, hvor det er muligt og krypteringsnøgler skal opbevares centralt i Keeper systemet. Det er ledelsens ansvar at sikre, at kryptografiske kontroller altid er relevante og up to date.

Fysisk sikring og miljøsikring

På adressen i Birkerød er der fysisk adgangskontrol der sikrer, at ikke alle kan komme ind.

Begge datacentre i Taastrup er perimeter sikret og det er kun muligt at komme hen til ejendommene ved brug af adgangskort med tilhørende kode. Der er få indgange, som er videoovervåget 24-7.

I forlængelse af dette har aimIT etableret retningslinjer og tilhørende tekniske foranstaltninger for at sikre, at medarbejderne arbejder hensigtsmæssigt. Disse tekniske foranstaltninger indebærer f.eks. automatisk skærmlås.

Driftssikkerhed

Driftsprocedurer og ansvarsområder
aimIT har via dokumentation og procesbeskrivelser, som løbende bliver opdateret, sikret sig at medarbejderne kan gå til opgaven uden at have erfaring med den enkelte kunde. Der er defineret klare processer for arbejdet i driftsmiljøet og en proces for ændringshåndtering sikrer, at ændringer sker efter aftale med kunder og er tilrettelagt hensigtsmæssigt i forhold til interne forhold. Der er ligeledes udarbejdet procedurer for logning og backup som er vigtige aspekter ved aimIT's ydelse.

I forlængelse af dette afholdes der jævnligt interne møder for opfølgning på driftsopgaver. Procedurerne og de tilknyttede politikker ligger tilgængeligt for samtlige relevante medarbejdere.

Kapacitetsstyring
Der er via generelle overvågningssystemer sat grænseværdier for, hvornår systemerne skal skaleres op af hensyn til elektronisk plads, svartider mv. Ligeledes, er der som tilknytning til denne, opsat alarmering der underretter aimIT om eventuelle kapacitetsproblemer. Det er driftsafdelingen der har til ansvar at følge op på disse alarmer.

Malwarebeskyttelse
aimIT har implementeret scannings- og overvågningssystemer til at sikre mod kendt skadevoldende kode, antivirus-systemer til overvågning af internetbrug og trafik og firewalls mv. til sikring af øvrigt tekniske og centrale installationer.

Backup
For at kunne genskabe systemer og data på hensigtsmæssig og korrekt vis er omfanget af backup formelt beskrevet i aftalerne med kunderne. aimIT har udarbejdet faste procedurer og beskrivelser for opsætning og vedligeholdelse af backup

Logning og overvågning

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

aimIT har etableret automatisk hændelseslogning på de anvendte systemer. Kun administratorer kan tilgå disse logs og de er ligeledes beskyttet mod manipulation. Driftsafdelingen har ansvaret for opretholdelsen af hændelseslogningen.

Styring af driftssoftware
Ændringer i driftsmiljøet sker i fastsatte servicevinduer og følger proceduren for ændringer. Kun autoriseret personale er i stand til at installere godkendt software på vores servere og medarbejdernes arbejdsstationer. Der er opsat software på aimIT endpoints og andre aktiver for at sige, at der konstant er styr på eventuelle tekniske sårbarheder (og at der sker en eventuel opfølgning på samme).

Der er opsat tekniske begrænsninger på software installationer. I tilfælde af, at almene medarbejdere hos aimIT forsøger at downloade uhensigtsmæssig software bliver anmodningen afvist.

Styring af netværkssikkerhed
Det er kun muligt at tilgå systemerne udefra med krypteret VPN-forbindelse med 2 faktor godkendelse. Der er ingen kunder, der kan tilgå vores systemer. De kunder, der er hostet i datacenteret, er beskyttet af separate firewalls. Således deler ingen kunder firewalls eller netværk.

Informationsoverførsel
Fortrolige informationer udveksles ikke via mails, uden at de – eller de medfølgende vedhæftede filer – er krypterede eller passwordbeskyttede. Der er udarbejdet regelsæt for håndtering af data og dokumenter. Reglerne er en del af it-sikkerhedspolitikken.

Leverandørforhold

Informationssikkerhed i leverandørforholdet
Hvor det er relevant, er der indgået databehandleraftaler med leverandører og der foreligger ikke nogen faste åbne adgange til nogen leverandører. Leverandøraftalerne blive nøje gennemgået ved indgåelse af en potentiel samarbejdsaftale med en leverandør.

Styring af leverandørydelser
Leverandørkontrakter, databehandleraftaler og revisor erklæringer vedligeholdes af ledelsen 1 gang årligt. Ledelsen sikrer som minimum at ledelsens retningslinjer stemmer overens med aimIT's politikker og opsatte foranstaltninger. I forlængelse af dette, vælger aimIT eventuelle leverandører efter eventuel risikovurdering for brugen af leverandørens ydelser.

Styring af informationssikkerhedsbrud og forbedringer

Ansvar og procedurer
Der er etableret procedurer for håndtering af sikkerhedshændelser og sikkerhedsbrud hos aimIT.

Der er formelt udpegede systemansvarlige, og kraven til de systemansvarlige er klart og formelt defineret. Den systemansvarlige skal udarbejde og vedligeholde procedurer, som sikrer rettidig og korrekt indgriben i forbindelse med sikkerhedsbrud. Der er fast procedure for håndtering af sikkerhedshændelser og sikkerhedsbrud.

Medarbejdere hos aimIT har til ansvar at indberette eventuelle sikkerhedssvagheder eller hændelser hvorefter ledelsen håndterer hændelsen/bruddet. Der er opsat en procedure for prioritering af hændelsen for at vurdere, om hændelsen reelt bør håndteres som et sikkerhedsbrud.

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Informationssikkerhedskontinuitet
aimIT har udarbejdet en formel og fast procedure til styring af beredskabsplanlægningen på alle niveauer. Der er implementeret formelle nødplaner og procedurer ved beredskab. Planen testes mindst én gang om året, så det sikres, at kunderne i mindst muligt omfang vil opleve forstyrrelser i driften i forbindelse med en eventuel nødsituation. Testen er ligeledes med til at planen konstant kan vedligeholdes og styrkes efter aktuelle trusler.

Overensstemmelse

Overensstemmelse stiller krav til kontroller til sikring mod brud på relevante IT-sikkerhedskrav.

Gennemgang af informationssikkerhed

Der afholdes løbende afdelingsmøder, hvor sikkerheden og procedurerne gennemgås. I forlængelse af dette har aimIT etableret interne kontroller for at sikre, at procedurerne bliver efterlevet hensigtsmæssigt. Nogle af de etablerede interne kontroller omhandler efterlevelse af ændringsstyringsproceduren og anti-malware. Disse kontroller er etableret for at sikre, at vores medarbejdere ikke afviger fra procedurer og politikker.

I forbindelse med udarbejdelse af de årlige ISAE 3402 erklæringer bliver der foretaget en evaluering fra en ekstern it-revisor.

Væsentlige ændringer i revisionsperioden

Der har ikke været nogle væsentlige ændringer i revisionsperioden.

Sektion 4: Kontrolmål, udførte kontroller, test og resultater heraf

Formål og omfang

Beskrivelse og resultat af vores tests af kontroller fremgår af efterfølgende skema. I det omfang vi ved vores test har konstateret afvigelser i design, implementering eller operationel effektivitet af de testede kontroller, har vi anført disse under resultat af test.

Denne erklæring er udarbejdet efter partielmetoden og aimIT A/S' kontrolbeskrivelse omfatter derfor ikke kontrolmål og tilknyttede kontroller hos aimIT A/S' underleverandør Curanet A/S og GlobalConnect.

Kontroller, som er specifikke for de enkelte kundeløsninger, eller som er udført af aimIT A/S' kunder, er ikke omfattet af vores erklæring.

Udførte test

Metoder anvendt til test af kontrollers funktionalitet er beskrevet nedenfor:

Metode	Overordnet beskrivelse
Forespørgsel	Forespørgsel af passende personale hos aimIT A/S. Forespørgsler har omfattet spørgsmål om, hvordan kontroller udføres.
Observation	Observation af kontrollens udførelse.
Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive operationelt effektive, hvis de implementeres. Desuden vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Derudover foretages der stikprøvevis test af kontrollernes operationelle effektivitet i revisionsperioden.
Genudførelse af kontrol	Vi har gentaget udførelse af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

Resultater af test

I nedenstående oversigt har vi opsummeret tests udført af Grant Thornton som grundlag for vurdering af de generelle it-kontroller hos aimIT A/S.

A.5 Informationssikkerhedspolitikker

A.5.1 Retningslinjer for styring af informationssikkerhed
Kontrolmål: At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.

Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
5.1.1	*Politikker for informationssikkerhed* Ledelsen har fastlagt og godkendt et sæt politikker for informationssikkerhed, som er offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter.	Vi har inspiceret, at informationssikkerhedspolitikken er godkendt af ledelsen, offentliggjort og kommunikeret til medarbejdere og relevante eksterne parter. Vi har inspiceret, at informationssikkerhedspolitikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.
5.1.2	*Gennemgang af politikker for informationssikkerhed* Politikkerne for informationssikkerhed gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Vi har forespurgt om proceduren for regelmæssig gennemgang af informationssikkerhedspolitikken. Vi har inspiceret, at informationssikkerhedspolitikken er evalueret med udgangspunkt i opdaterede risikovurderinger for at sikre, at den fortsat er egnet, fyldestgørende og effektiv.	Ingen afvigelser konstateret.

A.6 Organisering af informationssikkerhed

A.6.1 Intern organisering
Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
6.1.1	*Roller og ansvarsområder for informationssikkerhed* Alle ansvarsområder for informationssikkerhed defineres og fordeles.	Vi har inspiceret et organisationsdiagram for informationssikkerhedsorganisationen. Vi har inspiceret beskrivelse af roller og ansvarsområder i informationssikkerhedsorganisationen.	Ingen afvigelser konstateret.
6.1.2	*Funktionsadskillelse* Modstridende funktioner og ansvarsområder adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Vi har inspiceret dokumentation for adskillelse af funktioner. Vi har inspiceret overordnet organisationsdiagram for organisationen.	Ingen afvigelser konstateret.
6.1.4	*Kontakt med særlige interessegrupper* Der opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.	Vi har inspiceret dokumentation for, at der er opretholdt passende kontakt med særlige interessegrupper.	Ingen afvigelser konstateret.

A.6.2 Mobilt udstyr og fjernarbejdspladser Kontrolmål: At sikre fjernarbejdspladser og brugen af mobilt udstyr.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
6.2.1	*Politik for mobilt udstyr* Der er etableret en politik og understøttende sikkerhedsforanstaltninger til styring af de risici, der opstår ved anvendelse af mobilt udstyr.	Vi har inspiceret politikken for anvendelse af mobilt udstyr. Vi har stikprøvevis inspiceret, at der er implementeret tekniske kontroller til sikring af mobilt udstyr.	Ingen afvigelser konstateret.
6.2.2	*Fjernarbejdspladser* Der er implementeret en politik og understøttende sikkerhedsforanstaltninger for at beskytte information, der er adgang til, og som behandles eller lagres på fjernarbejdspladser.	Vi har inspiceret politik for sikring af fjernarbejdspladser. Vi har inspiceret underliggende sikkerhedsforanstaltninger til beskyttelse af fjernarbejdspladser.	Ingen afvigelser konstateret.

A.7 Medarbejdersikkerhed

A.7.1 Før ansættelsen
Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
7.1.1	*Screening* Efterprøvning af alle jobkandidaters baggrund udføres i overensstemmelse se med relevante love, forskrifter og etiske regler og står i forhold til de forretningsmæssige krav, klassifikationen af den information, der gives adgang til, og de relevante risici.	Vi har inspiceret procedure for screening af nye medarbejdere. Vi har inspiceret dokumentation for at der bliver indhentet screeningsdokumentation på nye medarbejdere.	Ingen afvigelser konstateret.
7.1.2	*Ansættelsesvilkår og -betingelser* Kontrakter med medarbejdere og kontrahenter beskriver de pågældendes og organisationens ansvar for informationssikkerhed.	Vi har inspiceret proceduren for ansættelse af nye medarbejdere. Vi har inspiceret dokumentation for at nye medarbejdere er blevet orienteret omkring deres roller samt ansvar ved informationssikkerhed.	Ingen afvigelser konstateret.

A.7.2 Under ansættelsen Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
7.2.1	*Ledelsesansvar* Ledelsen kræver, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Vi har inspiceret, at ledelsen har stillet krav om, at medarbejdere og kontrahenter skal overholde informationssikkerhedspolitikken.	Ingen afvigelser konstateret.
7.2.2	*Bevidsthed om, uddannelse og træning i informationssikkerhed* Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter vil ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour med organisationens politikker og procedurer, idet omfang det er relevant for deres jobfunktion.	Vi har inspiceret procedurer til sikring af tilstrækkelig uddannelse og træning i informationssikkerhed. Vi har inspiceret, at der er udført aktiviteter, der udbygger og vedligeholder sikkerhedsbevidstheden blandt medarbejderne.	Ingen afvigelser konstateret.
7.2.3	*Sanktioner* Der er etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.	Vi har inspiceret, at der er etableret en formel sanktionsproces, som er kommunikeret til medarbejdere og kontrahenter. Vi har inspiceret, at sanktionsprocessen er en del af ansættelseskontrakten.	Ingen afvigelser konstateret.

A.7.3 Ansættelsesforholdets ophør eller ændring Kontrolmål: At beskytte organisationens interesser som led i ansættelsesforholdets ophør eller ændring.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
7.3.1	*Ansættelsesforholdets ophør eller ændring* Informationssikkerhedsansvar og -forpligtelser, som gælder efter ansættelsens ophør eller ændring, defineres og kommunikeres til medarbejderen eller kontrahenten og håndhæves.	Vi har inspiceret dokumentation for at informationssikkerhedsansvar og -forpligtelser ved ansættelsens ophør eller ændring er defineret og kommunikeret. Vi har inspiceret, at fratrådte medarbejdere er bekendt med den stadigt gældende tavshedspligt ved fratrædelse.	Ingen afvigelser konstateret.

A.8 Styring af aktiver

A.8.1 Ansvar for aktiver
Kontrolmål: At identificere organisationens aktiver og definere passende ansvarsområder til beskyttelse heraf.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
8.1.1	*Fortegnelse over aktiver* Aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, og der udarbejdes og vedligeholdes en fortegnelse over disse aktiver.	Vi har inspiceret fortegnelsen over aktiver.	Ingen afvigelser konstateret.
8.1.2	*Ejerskab af aktiver* Der udpeges en ejer i organisationen for hvert aktiv.	Vi har inspiceret oversigt over ejerskab til aktiver.	Ingen afvigelser konstateret.
8.1.3	*Accepteret brug af aktiver* Regler for accepteret brug af information og aktiver i relation til information og informationsbehandlingsfaciliteter identificeres, dokumenteres og implementeres.	Vi har inspiceret reglerne for accepteret brug af aktiver.	Ingen afvigelser konstateret.
8.1.4	*Tilbagelevering af aktiver* Alle medarbejdere og eksterne brugere afleverer alle organisationsaktiver, der er i deres besiddelse, når deres ansættelse, kontrakt eller aftale ophører.	Vi har inspiceret procedure til sikring af tilbagelevering af udleverede aktiver. Vi har inspiceret, at aktiver er inddraget for fratrådte medarbejdere.	Ingen afvigelser konstateret.

A.8.3 Mediehåndtering Kontrolmål: at forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
8.3.2	*Bortskaffelse af medier* Medier bortskaffes på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.	Vi har inspiceret procedurer for bortskaffelse af medier. Vi har forespurgt, om der har været bortskaffelse af medier i revisionsperioden.	Vi er blevet informeret om, at medier ikke er blevet bortskaffet i revisionsperioden. Ingen afvigelser konstateret.

A.9 Adgangsstyring

A.9.1 Forretningsmæssige krav til adgangsstyring Kontrolmål: At begrænse adgangen til information og informationsbehandlingsfaciliteter.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
9.1.1	*Politik for adgangsstyring* En politik for adgangsstyring fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerhedskrav.	Vi har inspiceret politikken for adgangsstyring. Vi har inspiceret at politikken er gennemgået og godkendt af ledelsen.	Ingen afvigelser konstateret.
9.1.2	*Adgang til netværk og netværkstjenester* Brugere har kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Vi har inspiceret, at der er etableret en procedure for tildeling af adgang til netværk og netværkstjenester. Vi har inspiceret udtræk over brugere med adgang til netværk og netværkstjenester. Vi har forespurgt om adgange er tildelt baseret på medarbejdernes arbejdsbetingede behov.	Ingen afvigelser konstateret.

A.9.2 Administration af brugeradgang Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
9.2.1	*Brugerregistrering-og afmelding* Der er implementeret en formel procedure for registrering og afmelding af brugere med henblik på tildeling og afmelding af adgangsrettigheder.	Vi har inspiceret, at der foreligger formaliserede procedurer for tildeling og afmelding af brugernes adgangsrettigheder. Vi har stikprøvevis inspiceret, at brugernes adgangsrettigheder er godkendt. Vi har inspiceret, at fratrådte brugeres adgangsrettigheder er nedlagt.	Ingen afvigelser konstateret.
9.2.2	*Tildeling af brugeradgang* Der er implementeret en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har inspiceret, at der er etableret en procedure for brugeradministration. Vi har inspiceret, at tildelte brugeradgange til nyansatte medarbejdere er blevet tildelt efter proceduren for adgangsstyring.	Ingen afvigelser konstateret.
9.2.3	*Styring af privilegerede adgangsrettigheder* Tildeling og anvendelse af privilegerede adgangsrettigheder begrænses og styres.	Vi har inspiceret procedurerne for tildeling, anvendelse og begrænsning af privilegerede adgangsrettigheder. Vi har inspiceret, at der periodisk foretages gennemgang af privilegerede adgangsrettigheder.	Ingen afvigelser konstateret.
9.2.4	*Styring af hemmelig autentifikationsinformation om brugere* Tildeling af hemmelig autentifikationsinformation styres ved hjælp af en formel administrationsproces.	Vi har stikprøvevis inspiceret tildeling af passwords til platforme. Vi har inspiceret dokumentation for at password politikken er implementeret i anvendte systemer til styring af hemmelig autentifikationsinformation om brugere.	Ingen afvigelser konstateret.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
9.2.5	*Gennemgang af brugeradgangsrettigheder* Aktivejere gennemgår med jævne mellemrum brugernes adgangsrettigheder.	Vi har inspiceret procedure for regelmæssig gennemgang og evaluering af adgangsrettigheder. Vi har inspiceret, at der foretaget gennemgang og evaluering af adgangsrettigheder i revisionsperioden.	Ingen afvigelser konstateret.
9.2.6	*Inddragelse eller justering af adgangsrettigheder* Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter inddrages, når deres ansættelsesforhold, kontrakt eller aftale ophører, eller tilpasses efter en ændring.	Vi har inspiceret procedurerne for inddragelse og justering af adgangsrettigheder. Vi har inspiceret at fratrådte medarbejdere har fået deres adgangsrettigheder inddraget rettidigt.	Der er ikke modtaget dokumentation for, hvornår adgange er blevet inddraget for fratrådte medarbejdere. Ingen yderligere afvigelser konstateret.

A.9.3 Brugernes ansvar Kontrolmål: At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.			
Nr.	**aimIT A/S' kontrol**	**Grant Thorntons test**	**Resultat af test**
9.3.1	*Brug af hemmelig autentifikationsinformation* Brugere følger organisationens praksis ved anvendelse af hemmelig autentifikationsinformation.	Vi har inspiceret retningslinjer for brug af fortrolige passwords. Vi har inspiceret, at den implementerede passwordpolitik følger fastlagte retningslinjer.	Ingen afvigelser konstateret.

A.9.4 Styring af system- og applikationsadgang Kontrolmål: At forhindre uautoriseret adgang til systemer og applikationer.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
9.4.2	*Procedurer for sikker logon* Adgang til systemer og applikationer styres af en procedure for sikker logon.	Vi har inspiceret procedure for sikker logon. Vi har inspiceret, at der er implementeret MFA i forbindelse med logon.	Ingen afvigelser konstateret.
9.4.3	*System for administration af passwords* Systemer til administration af passwords er interaktive og sikrer passwords med god kvalitet.	Vi har inspiceret, at der i politikker eller procedurer stilles krav til kvaliteten af passwords. Vi har inspiceret, at systemer til administration af passwords er opsat i overensstemmelse med de stillede krav.	Ingen afvigelser konstateret.

A.10 Kryptografi

A.10.1 Kryptografiske kontroller Kontrolmål: At sikre korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
10.1.1	*Politik for anvendelse af kryptografi* Der er udarbejdet og implementeret en politik for anvendelse af kryptografi til beskyttelse af information.	Vi har inspiceret politik for anvendelse af kryptering. Vi har inspiceret oversigt over opdatering og gennemgang af politikker samt procedure, hvoraf politikken for kryptografi fremgår.	Ingen afvigelser konstateret.
10.1.2	*Administration af nøgler* Der er udarbejdet og implementeret en politik for anvendelse og beskyttelse af samt levetid for krypteringsnøgler gennem hele deres livscyklus.	Vi har inspiceret politikken for administration af nøgler, der understøtter virksomhedens brug af kryptografiske teknikker. Vi har inspiceret, at krypteringsnøgler er aktive samt at der følges op på hvornår de skal fornyes.	Ingen afvigelser konstateret.

A.11 Fysisk sikring og miljøsikring

A.11.1 Sikre områder
Kontrolmål: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
11.1.1	*Fysisk perimetersikring* Der er defineret og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og informationsbehandlingsfaciliteter.	Vi har inspiceret proceduren for fysisk beskyttelse af faciliteter og perimetersikkerhed. Vi har inspiceret relevante lokationer og deres perimetersikring for at konstatere, hvorvidt der er sikringsforanstaltninger til at forhindre uautoriseret adgang.	Ingen afvigelser konstateret.
11.1.2	*Fysisk adgangskontrol* Sikre områder er beskyttet med passende adgangskontrol for at sikre, at kun autoriseret personale kan få adgang.	Vi har inspiceret adgangspunkter for at konstatere, hvorvidt der anvendes personligt adgangskort til at opnå adgang til kontoret. Vi har inspiceret at der er opsat alarmsystemer til fysisk adgangskontrol.	Ingen afvigelser konstateret.

A.11.2 Udstyr
Kontrolmål: At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
11.2.6	*Sikring af udstyr og aktiver uden for organisationen* Der er etableret sikring af aktiver uden for organisationen under hensyntagen til de forskellige risici, der er forbundet med arbejde uden for organisationen.	Vi har inspiceret retningslinjer for sikring af udstyr og aktiver uden for organisationen.	Ingen afvigelser konstateret.
11.2.7	*Sikker bortskaffelse eller genbrug af udstyr* Alt udstyr med lagringsmedier verificeres for at sikre, at følsomme data og licensbeskyttet software er slettet eller forsvarligt overskrevet inden bortskaffelse eller genbrug.	Vi har inspiceret procedure for sletning af data og software på lagringsmedier inden bortskaffelse af lagringsmediet. Vi har stikprøvevis inspiceret at data og software er blevet slettet, før bortskaffelsen af udstyr fandt sted.	Ingen afvigelser konstateret.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
11.2.8	*Brugerudstyr uden opsyn* Brugere sikrer, at udstyr, som er uden opsyn, er passende beskyttet.	Vi har inspiceret proceduren for sikring af beskyttelse af udstyr, som er uden opsyn.	Ingen afvigelser konstateret.
11.2.9	*Politik for ryddeligt skrivebord og blank skærm* Der er udarbejdet en politik om at holde skriveborde ryddet for papir og flytbare lagringsmedier og om blank skærm på informationsbehandlingsfaciliteter.	Vi har inspiceret politik for ryddeligt skrivebord og blank skærm.	Ingen afvigelser konstateret.

A.12 Driftssikkerhed

A.12.1 Driftsprocedurer og ansvarsområder
Kontrolmål: At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
12.1.1	*Dokumenterede driftsprocedurer* Driftsprocedurer er dokumenteret og gjort tilgængelige for alle brugere, der har brug for dem.	Vi har inspiceret, at der er krav om, at driftsprocedurer skal være dokumenteret og vedligeholdt. Vi har inspiceret, at driftsdokumentation er opdateret og tilgængelig for medarbejdere, som har behov for dem.	Ingen afvigelser konstateret.
12.1.2	*Ændringsstyring* Ændringer af organisationen, forretningsprocesser, informationsbehandlingsfaciliteter og -systemer, som påvirker informationssikkerheden, styres.	Vi har inspiceret proceduren vedrørende ændringer til informationsbehandlingsudstyr og – systemer. Vi har stikprøvevis inspiceret dokumentation for at implementerede ændringer er håndteret i overensstemmelse med proceduren herfor.	Ingen afvigelser konstateret.
12.1.3	*Kapacitetsstyring* Anvendelsen af ressourcer overvåges og tilpasses, og der foretages fremskrivninger af fremtidige kapacitetskrav for at sikre, at systemet fungerer som krævet.	Vi har inspiceret proceduren for overvågning af anvendelse af ressourcer og tilpasning af kapacitet til sikring af opfyldelse af fremtidige kapacitetskrav. Vi har inspiceret, at relevante platforme er omfattet af proceduren for kapacitetsstyring.	Ingen afvigelser konstateret.

A 12.2 Malwarebeskyttelse Kontrolmål: At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.2.1	*Kontroller mod malware* Der er implementeret kontroller til detektering, forhindring og gendannelse for at beskytte mod malware, kombineret med passende brugerbevidsthed.	Vi har inspiceret retningslinjer for kontroller mod malware. Vi har inspiceret, at der er implementeret kontroller mod malware.	Ingen afvigelser konstateret.

A.12.3 Backup Kontrolmål: At beskytte mod tab af data.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.3.1	*Backup af information* Der tages backupkopier af information, software og systembilleder, og disse testes regelmæssigt i overensstemmelse med den aftalte backuppolitik.	Vi har inspiceret dokumentation for at proceduren for backup er gennemgået og opdateret i perioden. Vi har stikprøvevis inspiceret, at der tages backup jf. proceduren. Vi har inspiceret, at restoretest er gennemført.	Ingen afvigelser konstateret.

A.12.4 Logning og overvågning Kontrolmål: At registrere hændelser og tilvejebringe bevis.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.4.1	*Hændelseslogning* Hændelseslogning til registrering af brugeraktivitet, undtagelser, fejl og informationssikkerhedshændelser udføres, opbevares og gennemgås regelmæssigt.	Vi har forespurgt til logning af brugeraktivitet. Vi har inspiceret at logningskonfigurationerne indeholder brugeraktivitet, undtagelser, fejl og hændelser. Vi har forespurgt om logs er beskyttet mod manipulation.	Ingen afvigelser konstateret.
12.4.2	*Beskyttelse af log-oplysninger* Logningsfaciliteter og logoplysninger beskyttes mod manipulation og uautoriseret adgang.	Vi har forespurgt til procedurer for sikring af logoplysninger. Vi har inspiceret at logningsinformationer er beskyttet mod manipulation og uautoriseret adgang.	Ingen afvigelser konstateret.
12.4.3	*Administrator- og operatørlog* Aktiviteter udført af systemadministrator og systemoperatør logges, og loggen beskyttes og gennemgås regelmæssigt.	Vi har inspiceret procedurer vedrørende logning af aktiviteter udført af systemadministratorer og -operatører. Vi har stikprøvevis inspiceret at systemadministratorers og -operatørers handlinger logges på servere og databasesystemer.	Ingen afvigelser konstateret.
12.4.4	*Tidssynkronisering* Urene i alle relevante informationsbehandlingssystemer i en organisation eller et sikkerhedsdomæne er synkroniserede til en enkelt referencetidskilde.	Vi har inspiceret at der er implementeret synkronisering op imod en betryggende tidsserver.	Ingen afvigelser konstateret.

A.12.5 Styring af driftssoftware Kontrolmål: At sikre integriteten af driftssystemer.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.5.1	*Softwareinstallation på driftssystemer* Der er implementeret procedurer til styring af softwareinstallationen på driftssystemer.	Vi har inspiceret proceduren for patching og opgradering af systemer og at den er gennemgået og opdateret i perioden. Vi har inspiceret dokumentation for at relevante systemer er opdateret og patchet efter bestemte krav i proceduren herfor.	Ingen afvigelser konstateret.

A.12.6 Sårbarhedsstyring Kontrolmål: At forhindre, at tekniske sårbarheder udnyttes.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
12.6.1	*Styring af tekniske sårbarheder* Der indhentes løbende informationer om tekniske sårbarheder i anvendte informationssystemer, organisationens eksponering for sådanne sårbarheder skal evalueres, og der iværksættes passende foranstaltninger for at håndtere den tilhørende risiko.	Vi har inspiceret proceduren vedrørende indsamling og vurdering af tekniske sårbarheder. Vi har stikprøvevis inspiceret at servere, databasesystemer og netværkskomponenter er patchet rettidigt.	Ingen afvigelser konstateret.
12.6.2	*Begrænsninger på softwareinstallation* Der er fastlagt og implementeret regler om softwareinstallation, som foretages af brugerne.	Vi har inspiceret dokumentation for at der er begrænsninger for almene brugere på installation af software.	Ingen afvigelser konstateret.

A.13 Kommunikationssikkerhed

A.13.1 Styring af netværkssikkerhed
Kontrolmål: At sikre beskyttelse af informationer i netværk og af understøttende informationsbehandlingsfaciliteter.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
13.1.1	*Netværksstyring* Netværk styres og kontrolleres for at beskytte informationer i systemer og applikationer.	Vi har inspiceret, at der er defineret krav om styring og kontrol af netværk, herunder krav og regler om kryptering, segmentering, firewalls, intrusion detection og andre relevante sikkerhedsforanstaltninger. Vi har inspiceret dokumentation for design af netværket.	Ingen afvigelser konstateret.
13.1.3	*Opdeling af netværk* Grupper af informationstjenester, brugere og informationssystemer opdeles i netværk.	Vi har inspiceret netværksdiagrammer, hvoraf det fremgår at der er adskillelse af udviklings-, test- og driftsmiljøer. Vi har inspiceret teknisk dokumentation for at der er adskillelse af anvendte miljøer i systemer.	Ingen afvigelser konstateret.

A.13.2 Informationsoverførsel
Kontrolmålet: At opretholde informationssikkerhed ved overførsel internt i en organisation og til en ekstern entitet.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
13.2.3	*Elektroniske meddelelser* Informationer i elektroniske meddelelser beskyttes på passende måde.	Vi har inspiceret dokumentation for at meddelelser er sikret med passende opsætning af FTP-protokoller og ved brug af sikker mail.	Ingen afvigelser konstateret.

A.15 Leverandørforhold

15.2 Styring af leverandørydelser
Kontrolmål: At opretholde et aftalt niveau af informationssikkerhed og levering af ydelser i henhold til leverandøraftalerne.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
15.2.1	*Overvågning og gennemgang af leverandørydelser* Leverandørydelser overvåges, gennemgås og auditeres.	Vi har inspiceret, at proceduren for styring af leverandører og serviceaftaler indeholder krav til årlig overvågning og gennemgang af serviceydelser leveret af underleverandører, er i overensstemmelse med det aftalte. Vi har inspiceret, at der er foretaget gennemgang og vurdering af relevant revisionsrapportering på væsentlige underleverandører i perioden.	Ingen afvigelser konstateret.
15.2.2	*Styring af ændringer af leverandørydelser* Ændringer af leverandørydelser, herunder vedligeholdelse og forbedring af eksisterende informationssikkerhedspolitikker, - procedurer og -kontroller, styres under hensyntagen til, hvor kritiske de involverede forretningsinformationer, - systemer og -processer er, og til en revurdering af risici.	Vi har inspiceret procedurer for håndtering af ændringer af leverandørydelser. Vi har forespurgt til styring af ændringer hos leverandører.	Vi er blevet informeret om, at der ikke har været ændringer til leverandørydelser i perioden. Ingen afvigelser konstateret.

A.16 Styring af informationssikkerhedsbrud

A.16.1 Styring af informationssikkerhedsbrud og forbedringer
Kontrolmål: At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.

Nr.	*aimIT A/S' kontrol*	*Grant Thorntons test*	*Resultat af test*
16.1.1	*Ansvar og procedurer* Ledelsesansvar og procedurer er fastlagt for at sikre hurtig, effektiv og planmæssig håndtering af informationssikkerhedsbrud.	Vi har inspiceret proceduren for håndtering af sikkerheds-hændelser. Vi har inspiceret at proceduren er gennemgået og opdateret i perioden.	Ingen afvigelser konstateret.
16.1.2	*Rapportering af informationssikkerhedshændelser* Informationssikkerhedshændelser rapporteres ad passende ledelseskanaler så hurtigt som muligt.	Vi har inspiceret retningslinjer for rapportering af informati-onssikkerhedshændelser. Vi har stikprøvevis inspiceret at informationssikkerhedshæn-delser er rapporteret ad passende ledelseskanaler.	Ingen afvigelser konstateret.
16.1.3	*Rapportering af informationssikkerhedssvagheder* Medarbejdere og kontrahenter, som bruger orga-nisationens informationssystemer og -tjenester, har pligt til at notere og rapportere alle observe-rede svagheder eller mistanke om svagheder i in-formationssystemer og -tjenester.	Vi har inspiceret retningslinjer for rapportering af informati-onssikkerhedssvagheder. Vi har forespurgt om medarbejdere har rapporteret svaghe-der eller mistanke om svagheder i informationssystemer og -tjenester.	Vi er blevet informeret om, at der ikke har været rapporteret svagheder i revisionspe-rioden. Ingen afvigelser konstateret.
16.1.4	*Vurdering af og beslutning om informations- sik-kerhedshændelser* Informationssikkerhedshændelser vurderes, og det besluttes, om de skal klassificeres som infor-mationssikkerhedsbrud.	Vi har inspiceret procedure for vurdering af informationssik-kerhedshændelser. Vi har stikprøvevis inspiceret håndtering af informationssik-kerhedshændelser i revisionsperioden.	Ingen afvigelser konstateret.
16.1.5	*Håndtering af informationssikkerhedsbrud* Informationssikkerhedsbrud håndteres i overens-stemmelse se med de dokumenterede procedurer.	Vi har inspiceret proceduren for håndtering af informations-sikkerhedsbrud. Vi har forespurgt om der har været informationssikkerheds-brud i perioden.	Vi er blevet informeret om, at der ikke har været informationssikkerhedsbrud i revisi-onsperioden. Ingen afvigelser konstateret.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
16.1.6	*Erfaring fra informationssikkerhedsbrud* Den viden, der opnås ved at analysere og håndtere informationssikkerhedsbrud, anvendes til at nedsætte sandsynligheden for eller virkningen af fremtidige brud.	Vi har forespurgt hvordan erfaringer fra informationssikkerhedsbrud håndteres. Vi har forespurgt om der har været informationssikkerhedsbrud i perioden.	Vi er blevet informeret om, at der ikke har været informationssikkerhedsbrud i revisionsperioden. Ingen afvigelser konstateret.

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

A.17.1 Informationssikkerhedskontinuitet
Kontrolmål: At sikre, at informationssikkerhed er forankret i organisationens ledelsessystemer for nød-, beredskabs- og reetableringsstyring.

Nr.	aimIT A/S' kontrol	Grant Thorntons test	Resultat af test
17.1.1	*Planlægning af informationssikkerhedskontinuitet* Organisationen har fastlagt krav til informationssikkerhed og informationssikkerhedskontinuitet i kritiske situationer, f.eks. i tilfælde af en krise eller katastrofe.	Vi har inspiceret at beredskabsplanen er godkendt af ledelsen.	Ingen afvigelser konstateret.
17.1.2	*Implementering af informationssikkerhedskontinuitet* Organisationen har fastlagt, dokumenteret og implementeret processer, procedurer og kontroller for at sikre den nødvendige informationssikkerhedskontinuitet i en kritisk situation og disse vedligeholdes.	Vi har inspiceret at beredskabsplanen vedligeholdes og opdateres efter behov. Vi har inspiceret dokumentation for at beredskabsplanen er tilgængelig for relevante medarbejdere.	Ingen afvigelser konstateret.
17.1.3	*Verificer, gennemgå og evaluer informationssikkerhedskontinuiteten* Organisationen verificerer de etablerede og implementerede kontroller vedrørende informationssikkerhedskontinuiteten med jævne mellemrum med henblik på at sikre, at de er tidssvarende og effektive i kritiske situationer.	Vi har inspiceret dokumentation for at der er udført tests af beredskabsplanens risikoområder i perioden.	Ingen afvigelser konstateret.

A.17.2 Redundans Kontrolmål: At sikre tilgængelighed af informationsbehandlingsfaciliteter.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
17.2.1	Tilgængelighed af informationsbehandlingsfaciliteter Informationsbehandlingsfaciliteter er implementeret med tilstrækkelig redundans til at kunne imødekomme tilgængelighedskrav.	Vi har inspiceret tilkøb af etablering af redundans til sikring af tilgængelighed af driftssystemer.	Ingen afvigelser konstateret.

A.18 Overensstemmelse

A.18.2 Gennemgang af informationssikkerheden Kontrolmål: At sikre, at informationssikkerhed er implementeret og drives i overensstemmelse med organisationens politikker og procedurer.			
Nr.	***aimIT A/S' kontrol***	***Grant Thorntons test***	***Resultat af test***
18.2.1	*Uafhængig gennemgang af informationssikkerhed* Organisationens metode til styring af informationssikkerhed og implementeringen heraf (dvs. kontrolmål, kontroller, politikker, processer og procedurer for informationssikkerhed) gennemgås uafhængigt med planlagte mellemrum eller i tilfælde af væsentlige ændringer.	Vi har inspiceret dokumentation for at der er foretaget uafhængig gennemgang af informationssikkerheden.	Ingen afvigelser konstateret.
18.2.2	*Overensstemmelse med sikkerhedspolitikker og sikkerhedsstandarder* Lederne undersøger regelmæssigt, om informationsbehandlingen og -procedurerne inden for deres ansvarsområde er i overensstemmelse med relevante sikkerhedspolitikker, standarder og andre sikkerhedskrav.	Vi har stikprøvevis inspiceret dokumentation for at de interne kontroller vedrørende overholdelse af politikker og procedurer er blevet udført.	Ingen afvigelser konstateret.