Deloitte.

Nianet A/S

ISAE 3402 Type 2

Erklæring om fysisk sikring og effektiviteten heraf for perioden fra 16. juni 2016 til 15. juni 2017

Indholdsfortegnelse

1 Uafhængig revisors erklæring

Til ledelsen i Nianet A/S

Omfang
Vi har fået til opgave at erklære os om Nianet A/S' (herefter Nianet) beskrivelse på side 6-12 om håndteringen af de generelle it-kontroller omfattende design, implementering og effektivitet af kontroller i relation til de kontrolmål, som er anført i beskrivelsen.

Beskrivelsen og dermed vores erklæring omhandler udelukkende fælles processer, kontrollerne heri samt security baselines, som er generelt gældende for Nianets kunder. For kunder, som har specifikke krav til processer og til sikkerhed, vil nærværende erklæring ikke være dækkende.

Nianets ansvar
Nianet er ansvarlig for udarbejdelse af beskrivelse og medfølgende ledelsesudtalelse på side 4-5, herunder fuldstændigheden, nøjagtigheden og den måde, hvorpå beskrivelsen og udtalelsen er præsenteret, for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for design, implementering og effektivt fungerende kontroller med henblik på at nå de anførte kontrolmål.

Revisors ansvar
Det er vores ansvar, baseret på vores procedurer, at udtrykke en konklusion om Nianets beskrivelse samt om design, implementering og effektivitet af kontroller relateret til de kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE3402 Erklæringer med sikkerhed om kontroller hos serviceleverandører, som er udstedt af IAASB. Denne standard kræver, at vi opfylder etiske krav samt planlægger og udfører vores handlinger med henblik på at opnå en høj grad af sikkerhed for, at beskrivelsen i alle væsentlige henseender er dækkende, og at kontrollerne er hensigtsmæssigt designet og fungerer effektivt.

Vi har overholdt kravene til uafhængighed og andre etiske krav i IESBA's Etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

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

En erklæringsopgave med sikkerhed, hvor der afgives erklæring om beskrivelsen, udformningen og effektiviteten af kontroller hos Nianet, omfatter udførelse af handlinger med henblik på at opnå bevis for oplysningerne i Nianets beskrivelse af sit system samt for kontrollernes udformning og effektivitet. De valgte handlinger afhænger af 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 en test af effektiviteten af de kontroller, som vi anser som nødvendige for at opnå en høj grad af sikkerhed for, at de kontrolmål, der er anført i beskrivelsen, blev nået. En erklæringsopgave med sikkerhed af denne type omfatter endvidere vurdering af den samlede præsentation af beskrivelsen, hensigtsmæssigheden af de heri anførte mål samt hensigtsmæssigheden af de kriterier, som Nianet har specificeret og beskrevet i sektion 2 og 3.

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

Begrænsninger i en virksomheds kontroller
Kontroller hos en serviceleverandør kan i sagens natur ikke forhindre eller opdage alle fejl eller udeladelser ved behandling eller rapportering af transaktioner. Herudover er fremskrivning af systembeskrivelse og konklusion udsat for den risiko, at kontroller hos en serviceleverandør kan blive utilstrækkelige eller svigte.

Konklusion
Vores konklusion er udformet på grundlag af de forhold, der er beskrevet i denne erklæring. De kriterier, som vi har anvendt ved udformningen af konklusionen, er beskrevet på side 9. Det er vores opfattelse:

1) at beskrivelsen af Nianets ydelser og kontrolmiljø, således som de var designet og implementeret i perioden fra 16. juni 2016 til 15. juni 2017, i alle væsentlige henseender er dækkende.
2) at de kontroller, som knytter sig til de kontrolmål, der er anført i beskrivelsen, har været hensigtsmæssigt designet i perioden fra 16. juni 2016 til 15. juni 2017.
3) at 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 fungeret effektivt i hele perioden fra 16. juni 2016 til 15. juni 2017.

Ovenstående konklusion dækker ikke kundespecifikke krav til procedurer og sikkerhed i kontraktgrundlaget samt overholdelse af de specifikke krav i lov om behandling af personoplysninger (Persondataloven). Såfremt kunder ønsker en erklæring om kundespecifikke forhold, skal der indgås aftale med Nianet om udarbejdelse af kundespecifikke erklæringer.

Beskrivelse af test af kontroller
De specifikke, testede kontroller samt karakteren og resultatet af disse test fremgår af sektion 4.

Tiltænkte brugere og formål
Denne erklæring og beskrivelsen af kontroltest i sektion 4 er kun tiltænkt Nianet, Nianets kunder og deres revisorer, som har en tilstrækkelig forståelse herfor til at tage erklæringens indhold i betragtning tillige med anden information, herunder information om kundens egne kontroller, når risikoen for væsentlig fejlinformation i årsregnskaber skal vurderes.

København, den 21.06.2017

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Jesper Due Sørensen
partner, CISA

Thomas Kühn
statsautoriseret revisor

2 Udsagn fra Nianet

Den i sektion 3 anførte beskrivelse er udarbejdet til brug for Nianets kunder, der har anvendt Nianet som driftsleverandør, og deres revisorer, som har en tilstrækkelig forståelse til at kunne 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. Nianet bekræfter, at:

(a) den medfølgende beskrivelse i sektion 3 giver en dækkende beskrivelse af Nianets driftsydelser, som leveres til kunderne for perioden fra 16. juni 2016 til 15. juni 2017. De kriterier, som dette udsagn baseres på, er, at den medfølgende beskrivelse:

(I) redegør for, hvordan systemet er designet og implementeret, herunder redegør for:
- de typer af ydelser, der er leveret.
- processer for it-anvendelsen omfattende sikring af fortrolighed, integritet og tilgængelighed af systemer og data.
- den proces, der anvendes til at udarbejde rapporter og anden information til kunder.
- relevante kontrolmål og kontroller udformet til at nå disse mål.
- de kontroller, som vi med henvisning til systemets udformning har forudsat ville være implementeret af Nianets 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.
- 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 driftsydelser til Nianets kunder.

(II) indeholder relevante oplysninger om ændringer i Nianets system foretaget i perioden fra 16. juni 2016 til 15. juni 2017.

(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 for vigtigt efter deres særlige forhold.

(b) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, er hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 16. juni 2016 til 15. juni 2017. Kriterierne for dette udsagn er, at:

(I) de risici, der truer opnåelsen af de kontrolmål, der er anført i beskrivelsen, er identificeret.

(II) de identificerede kontroller vil, hvis anvendt som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrer opnåelsen af de anførte kontrolmål.

(III) kontrollerne er anvendt konsistent som udformet, herunder er manuelle kontroller blevet udført af personer med passende kompetence og beføjelse i hele perioden fra 16. juni 2016 til 15. juni 2017.

Glostrup, den 21.06.2017

Nianet

Rasmus Helmich
CEO

Per Skovgaard Rosen
CTO

3 Systembeskrivelse fra Nianet

3.1 Introduktion

Denne beskrivelse er udfærdiget med henblik på at levere information til brug for Nianets kunder og disses revisorer og for at opfylde kravene i ISAE 3402-erklæringer med sikkerhed om kontroller hos en serviceleverandør. Beskrivelsen er ligeledes udfærdiget med det formål at give information omkring de kontroller, der anvendes i forhold til levering af datakommunikationsløsninger og co-location leveret af Nianet.

Omfang
I beskrivelsen gives der oplysninger om de kontroller, der anvendes i forbindelse med fysisk sikkerhed omkring de ydelser, der leveres af Nianet. Beskrivelsen omfatter fysisk sikkerhed, som leveres af Nianet, og fokuserer på de kontrolmål, der er relevante for de interne kontroller, som relaterer sig til regnskabsaflæggelsen for Nianets kunder. Beskrivelsen omfatter de forretningsprocesser, som Nianet har fastslået som værende væsentlige for deres kunder ud fra et regnskabsmæssigt synspunkt, tillige med de understøttende, generelle it-kontroller. Ledelsen i Nianet er ansvarlig for at identificere kontrolmål og for de manuelle og automatiske kontroller, der er sat i drift med henblik på at opnå disse mål. Dette inkluderer den informationsteknologi og infrastruktur, der understøttes af Nianets driftsorganisation.

Beskrivelsen er udarbejdet med henblik på at omfatte størstedelen af Nianets kunder. Derfor vil der blive fokuseret på de processer og kontroller, der anvendes i de fælles processer. Specifikke kundeforhold samt kontroller i forbindelse med specifikke krav i lov om behandling af personoplysninger (Persondataloven) er ikke omfattet af denne beskrivelse.

Beskrivelse af Nianet
Nianet er et it-driftsselskab (informations- og kommunikationsteknologi) med fokus på datakommunikationsløsninger baseret på fiber til offentlige og private erhvervsvirksomheder. Nianet er blandt de største udbydere på det danske marked. Nianet er landsdækkende og ejer fiber til mere end 3.500 unikke adresser via mange tusind kilometer fiber. Nianet er etableret i maj 2003 og ejes af 14 danske energiselskaber fordelt over hele landet.

It-ydelser
Nianet leverer datakommunikationsløsninger, co-location samt cloud-løsninger.

Vores ydelser inkluderer bl.a.:

- MPLS VPN
- Internettrafik
- Managed LAN
- Sort og grå fiber
- DSL-forbindelse
- Internationale forbindelser
- Co-location/Housing
- Private Cloud, Virtuel Server og Backup as a Service (BaaS)
- Hosted Firewall og nextgen firewall
- Anti DDoS-løsninger
- Hardware- og software-VPN.

Denne beskrivelse omfatter dog kun de kontrolaspekter, som relaterer sig til fysisk sikkerhed, risikostyring og beredskab, og har til formål at efterleve ISO27001 for co-location og netværkskunder.

Kriterier
Følgende generiske informationer og kontrolkriterier er anvendt til at udarbejde den overordnede system- og kontrolbeskrivelse med henblik på at vurdere, hvorvidt kontrollerne er udformet på passende vis, og vurdere, hvorvidt kontrollerne fungerer effektivt. Disse kriterier er inspireret af den internationale kontrolstandard ISO/IEC 27001 (Informationssikkerhed) og er baseret på Lov om net- og

informationssikkerhed og de fire bekendtgørelser, som regulerer NIS-loven, samt forretningsmæssige krav i de ydelser, Nianet tilbyder, herunder:

- Fysisk og logisk sikring
- Risikostyring
- Beredskab.

3.2 Kontrolmiljø, risikovurdering og monitorering

Nianets kontrolmiljø reflekterer den stilling, som ledelsen har taget til betydningen af kontroller og den vægt, der lægges på kontroller i politikker, procedurer, metoder og den organisatoriske struktur. Følgende er en beskrivelse af Nianets kontrolmiljø og Nianets leverancer af it-ydelser:

- Ansvar, Nianets direktion og bestyrelse
- Nianets organisationsstruktur
- Risikostyring.

3.2.1 Ansvar, Nianets bestyrelse og direktion

Nianet ejes af 14 danske energiselskaber, der har indsat en bestyrelse bestående af:

- Bestyrelsesformand Rune Nygaard Bech Pedersen
- Seks menige bestyrelsesmedlemmer
- Fire medarbejdervalgte medlemmer.

Nianets bestyrelse mødes mindst en gang per kvartal for at drøfte:

- Forretningsplaner og -strategi
- Økonomiske resultater
- Observationer og anbefalinger
- Resultater fra ekstern revision, når disse foreligger.

Nianets direktion har det ultimative ansvar for at overholde Nianets forretningspolitikker. Nianets direktion mødes ugentligt, og her drøftes visse strategiske oplæg og alle spørgsmål af taktisk og operationel karakter, overordnede politikker og overordnede processer – altså helt almindelig daglig ledelse af en virksomhed i stærk vækst med 120 medarbejdere.

Nianets direktion ser ud som følger:
Administrerende direktør – Rasmus Helmich
Økonomidirektør – Søren Fæster Nielsen
Salgsdirektør og marketingdirektør – Peter Sandahl Torp
Leverancedirektør – Mette Slesvig
Teknisk direktør – Per Skovgaard Rosen.

Fysisk er Nianet placeret med hovedkontor i Glostrup og en afdeling i Skanderborg samt fem datacentre i henholdsvis Glostrup, Taastrup, Vallensbæk, Skanderborg og Århus.

3.3 Risikostyring

Risikovurdering
Ledelsen mødes regelmæssigt for at drøfte forretningsrisici, inklusive økonomiske og teknologiske risici. Tillige mødes alle ledere regelmæssigt med personalet for at drøfte udeståender i forbindelse med teamets arbejde.

På årsbasis gennemfører Nianets sikkerhedsorganisation en risikovurdering af Nianets aktiver på baggrund af ISO/IEC 27005. Den anvendte model til vurdering af risici omfatter en vurdering af konsekvens, sandsynlighed og sårbarheder. Processen tager både eksterne og interne faktorer og trusler med i betragtning tillige med ledelsens evne til at fokusere på disse faktorers påvirkning af driften.

Risikoanalysen indeholder risikoejerspecificering, ledelsesvurdering og håndtering af risiko.

It-sikkerhedspolitik og sikringsplaner
Der er på baggrund af risikovurderingen og sårbarhedsanalysen udarbejdet it-sikkerhedspolitik og sikringsplaner. It-sikkerhedspolitikken og relevante sikringsplaner er udarbejdet for at imødegå identificerede risici.

Sikringsplaner inkluderer planer til sikring af, at særligt kritiske dele af virksomhedens infrastruktur, herunder datacentre og større POPs (Point-Of-Presence), har en lav sårbarhed. Sikringsplaner testes i henhold til fastlagt og godkendt testplan. It-sikkerhedspolitikken og sikringsplanerne revurderes årligt i forbindelse med den årlige risikoanalyse samt testplanernes resultater.

Persondatasikkerhed
Nianet har på baggrund af risikoanalyse og krav i Lov om net- og informationssikkerhed udarbejdet en persondatasikkerhedspolitik. Persondatasikkerhedspolitikken opdateres mindst en gang årligt i forbindelse med risikoanalysen samt ved pludseligt opståede krav eller hændelser, der kræver opdatering.

Eksterne leverandører
Nianet kræver på baggrund af Lov om net- og informationssikkerhed, at alle underleverandører efterlever de stillede krav. Nianet har udarbejdet en formel aftale, der specificerer krav til efterlevelse. Alle leverandører skal have underskrevet en aftale.

Overvågning og kommunikation
Nianet overvåger og registrerer brud på it-sikkerheden og persondatasikkerheden gennem en formelt dokumenteret incident management-proces. Alle hændelser registreres og dokumenteres i et sagsstyringssystem. Registrering af og dokumentation for hændelser gemmes i systemet og ved backup uden tidsbegrænsning.

Ved hændelser, herunder brud på persondatasikkerheden og identificering af særlige trusler, informeres slutbrugere og styrelser i henhold til relevante bekendtgørelser omfattet af NIS-loven gennem en incident management-proces. Alle hændelser af høj prioritet rapporteres gennem processen til CTO, der er ansvarlig for at informere og rapportere til slutbrugere, kunder og offentlig myndighed.

Påbud og informationer fra styrelsen overvåges hos Nianet af kontaktpunktet hos offentlig myndighed samt af CTO.

Overvågning af ekstern revision
Nianet er genstand for regelmæssige reviews foretaget af eksterne revisorer. Anbefalinger fra eksterne revisorer angående interne kontroller bliver taget til behørig efterretning.

3.4 Beredskab

Beredskabs- og kriseplaner
Nianet har på baggrund af årligt udførte risikovurderinger udarbejdet og implementeret en beredskabspolitik og beredskabsplaner til efterlevelse af BEK 564 og 567. Beredskabsplanerne og politikken indeholder sikring af alle de områder, der er specificeret i bekendtgørelser og den udarbejdede risikovurdering. Nianet har udarbejdet beredskabsplaner for fysisk skade på alle væsentlige lokationer og en krisehåndteringsplan, der er fælles for alle større hændelser, herunder større trusler i henhold til BEK 567.

Beredskabsplaner revurderes årligt i forbindelse med risikoanalysen.

Beredskabsøvelser
Nianet har på baggrund af krav i BEK 567 § 35 udarbejdet en femårig testplan, der indeholder beredskabstest af alle væsentlige dele af beredskabet. Testplanen revurderes årligt i forbindelse med revurderingen af beredskabsplaner.

Overvågning og kommunikation
Nianet overvåger og registrerer brud på it-sikkerheden, herunder beredskabshændelser og krisehåndtering, gennem en formelt dokumenteret incident management-proces. Alle hændelser registreres og dokumenteres i et sagsstyringssystem. Registrering af og dokumentation for hændelser gemmes i systemet og ved backup uden tidsbegrænsning.

Ved hændelser informeres slutbrugere og styrelser i henhold til BEK 566 (Bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed) gennem en incident management-proces. Alle hændelser af høj prioritet rapporteres gennem processen til CTO, der er ansvarlig for at informere og rapportere til slutbrugere, kunder og offentlig myndighed.

Påbud og informationer fra offentlig myndighed overvåges hos Nianet af kontaktpunkt til styrelsen samt af CTO.

3.5 Sikkerhed

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

Sikkerhed, fysisk adgang
Nianet A/S har etableret formelle politikker og procedurer for kontrol af adgang til systemer, faciliteter og datacentre. Disse politikker og procedurer definerer de niveauer af adgang, der er tilladt i henhold til klassificeringen af medarbejdere, og beskriver de tiltag og tilladelser, der kræves for at opnå og overvåge adgang.

Administration af adgangskontrol
Datacenterindgange er sikret af elektroniske læsere af adgangskort, som er forbundet med en central computer. Adgangen til datacentre administreres ud fra jobansvar af Nianets Network Operations Center (NOC). Der er krav om, at kunden giver oplysninger om det niveau af adgange, der ønskes, tillige med behørig tilladelse, før adgangskort udarbejdes og udleveres. Der udstedes personlige adgangskort med tilhørende personlig adgangskode. Eksterne brugere med adgang til datacentre har udelukkende adgang til eget aflåst rackskab eller område.

Administration af brugeradgang til systemer og data
Der er udarbejdet en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde adgangsrettigheder for alle brugertyper til alle systemer og data. It-sikkerhedshåndbogen beskriver endvidere kravene til Nianets medarbejdere i relation til adgange. Brugere tildeles kun adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte. Ved fratrædelse fratages brugerne deres adgangsrettigheder til systemer og data.

Overvågning
Adgange til datacentre er udstyret med alarmer og overvåges med videokameraer. Videoaktivitet overføres til en central server. Sikkerhedspersonalet undersøger aktivering af døralarmer. Sikkerhedsvagter konfronterer alle uautoriserede eller mistænkelige personer, som forsøger at få adgang uden for normal arbejdstid. Derudover er al adgang til datacentre overvåget, således at kontrolleret/autoriseret adgang opretholdes, og hvor det er nødvendigt, bliver entreprenører, der har behov for at servicere udstyr i datacentre, eskorteret.

Fysiske sikringsforanstaltninger
Datacentre er opført i henhold til Uptime Tier2- eller Tier3-definition. Datacentre forsynes af den lokale el-distributør og gennem standby-generatorer og via redundant UPS-anlæg, som sikrer stabil elforsyning ved nedbrud på offentlig forsyning. Ved svigt i offentlig elforsyning starter generatorer (typisk 500-1000 KVA dieselgeneratorer) automatisk op og sikrer den fortsatte elforsyning. Generatorerne testes kvartalsvis, og UPS testes regelmæssigt – alt i øvrigt i henhold til sikringsplaner.

Køling af rackskabe i datacentre sker under hævede edb-gulve. Køleanlægget sørger for, at kølig, filtreret luft "skubbes" op gennem rackskabet nedefra. I Nianets datacentre anvendes som oftest kuber, hvor kold luft forsynes i "kolde gange", og varm luft fra udstyr blæses ud i de omgivende rum, hvorfra et

køleaggregat opsuger den opvarmede luft og via kølevand afsætter kalorier i udendørs enheder. Alle områder og rackskabe har en temperatur på maksimalt 25° C og en luftfugtighed på maksimalt 60 %.

De områder, hvor der er opstillet udstyr, er opført i brandhæmmende materiale. Datacentre er beskyttet af Argonite- eller Inergen-anlæg, der er koblet til brandmeldeanlæg. Der er tilkoblet optiske og ioniserende røgalarmer i både loft og under det hævede gulv i lokalerne. Disse overvåger konstant områderne og afgiver endvidere audiovisuel alarm.

Ved alarmering via to eller flere meldeanlæg udløses slukningsanlæg i det pågældende rum. Samtidig sendes alarmen videre til kontrolcentralen.

Området er videoovervåget, og al aktivitet logges.

Datacentre er S40-certificerede.

3.6 Brugerkontrol – hensyn til kunder

Nianet A/S' kontroller er designet ud fra den antagelse, at visse interne kontroller er implementeret hos kunderne/brugerne. Implementeringen af sådanne interne kontroller er nødvendig for at opnå de kontrolmål, som er beskrevet i sektion 4. Der kan være yderligere kontrolmål og relaterede kontroller hos brugere, som kan være hensigtsmæssige for transaktioner, og som ikke er angivet i denne beskrivelse.

Dette afsnit beskriver visse kontroller, som brugere hos leverandøren har implementeret for at opnå de kontrolmål, der er angivet i beskrivelsen. De kontrolovervejelser, som er anført nedenfor, skal ikke ses som en fyldestgørende liste over de kontroller, der skal anvendes af brugere:

Adgangskontrol: Kunden har selv ansvaret for at etablere kontroller, der sikrer, at egne brugere oprettes og nedlægges i overensstemmelse med de af kunden vedtagne procedurer for at begrænse uautoriseret adgang. Kontrollen bør indeholde foranstaltninger, der sikrer periodisk review af adgangstilladelse til brugere med henblik på at sikre, at adgang fortsat er hensigtsmæssig på baggrund af brugeransvar og sikkerhedskrav.

4 Information distribueret af Deloitte

4.1 Introduktion

Denne oversigt er udformet med henblik på at informere Nianets kunder om de etablerede systemer og kontroller, som kan påvirke behandlingen af forretningsrelaterede transaktioner, og samtidig informere brugerne om effektiviteten af de kontroller, der blev efterprøvet. Afsnittet, når det kombineres med en forståelse og vurdering af kontrollerne i virksomhedens forretningsprocesser, har til hensigt at hjælpe Nianets kunders revisorer i (1) planlægningen af revisionen af virksomhedens årsregnskaber og (2) vurderingen af risici for fejl i virksomhedens årsregnskaber, som muligvis påvirkes af kontrollerne hos Nianet.

Vores test af Nianets kontroller er begrænset til de kontrolmål og relaterede kontroller, som er nævnt i nedenstående kontrolmatrix i denne del af rapporten, og er ikke udvidet til at omfatte alle de kontroller, der er beskrevet i Nianets systembeskrivelse, eller til kontroller, som muligvis er implementeret i brugerorganisationerne. Det er hver enkelt kunderevisors ansvar at vurdere denne information i forhold til de kontroller, som eksisterer i brugerorganisationen.

Overordnet kontrolmiljø
I tillæg til test af kontrollernes effektivitet som angivet i kontrolmatrixen i denne del af rapporten har vi foretaget test af Nianets overordnede kontrolmiljø, inklusive risikostyring.

Vores test af kontrolmiljøet inkluderede forespørgsler til relevante ledere, tilsynsførende og personale samt inspektion af Nianets dokumenter og registreringer. Kontrolmiljøet er vurderet med henblik på at bestemme karakteren, timingen og omfanget af kontrollers effektivitet.

4.2 Test af effektivitet

Vores test af kontrollers effektivitet inkluderer de test, som vi betragter som nødvendige for at vurdere, hvorvidt de udførte kontroller og overholdelsen heraf er tilstrækkelige til at give en høj, men ikke absolut, overbevisning om, at de specificerede kontrolmål blev opnået i perioden fra 16. juni 2016 til 15. juni 2017. Vores test af kontrollernes effektivitet er udformet til at dække et repræsentativt antal af transaktioner i løbet af perioden fra 16. juni 2016 til 15. juni 2017 for hver kontrol, jf. nedenfor, som er designet til at opnå de specifikke kontrolmål. I udvælgelsen af specifikke test har vi overvejet (a) karakteren af de testede områder, (b) typerne af tilgængelig dokumentation, (c) karakteren af de revisionsmål, der skal opnås, (d) det vurderede kontrolrisikoniveau og (e) testens forventede effektivitet.

4.3 Sikkerhed, kontrolmål og kontrolaktiviteter

4.3.1 A.5.1. Informationssikkerhedspolitikker (ISO 27001)

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål: At give retningslinjer for og understøtte informationssikkerhed i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter. DS/ISO IEC 27002:2014				
A.5.1.1	Politiker for informationssikkerhed Ledelsen skal fastlægge og godkende et sæt politikker for informationssikkerhed, som skal offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.	Ingen	Vi har påset, at der foreligger en ledelsesgodkendt it-sikkerhedspolitik, og at denne er tilgængelig på intranettet. Yderligere har vi påset, at denne gennemgås årligt for at sikre tilstrækkelighed.	Ingen væsentlige bemærkninger
A.5.1.2	Gennemgang af politikkerne for informationssikkerhed Politikkerne for informationssikkerhed skal gennemgås med planlagte mellemrum eller i tilfælde af væsentlige ændringer for at sikre deres fortsatte egnethed, tilstrækkelighed og resultatrelaterede effektivitet.	Ingen	Se A.5.1.1	Ingen væsentlige bemærkninger

4.3.2 A.6.1. Intern organisering (ISO 27001)

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål: At etablere et ledelsesmæssigt grundlag for at kunne igangsætte og styre implementeringen og driften af informationssikkerhed i organisationen. DS/ISO IEC 27002:2014				

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
A.6.1.1	Roller og ansvarsområder for informationssikkerhed Alle ansvarsområder for informationssikkerhed skal defineres og fordeles.	Ingen	Vi har påset dokumentationen for, at der er etableret en it-sikkerhedsorganisation, som definerer organisationens ansvar, samt en beskrivelse af de forskellige medlemmers roller.	Ingen væsentlige bemærkninger
A.6.1.2	Funktionsadskillelse Modstridende funktioner og ansvarsområder skal adskilles for at nedsætte muligheden for uautoriseret eller utilsigtet anvendelse, ændring eller misbrug af organisationens aktiver.	Ingen	Vi har påset, at der er etableret processer, der skal sikre funktionsadskillelse ved, at nærmeste leder skal udfylde en formular, hvor det skal defineres, hvilke fysiske og systemmæssige adgange den enkelte medarbejder skal have.	Ingen væsentlige bemærkninger
A.6.1.3	Kontakt med myndigheder Der skal opretholdes passende kontakt med relevante myndigheder.	Ingen	Vi har indhentet dokumentation for, at der er oprettet kontaktpunkt til projektenheden for cybersikkerhed.	Ingen væsentlige bemærkninger
A.6.1.4	Kontakt med særlige interessegrupper Der skal opretholdes passende kontakt med særlige interessegrupper eller andre faglige sikkerhedsfora og faglige organisationer.	Ingen	Se A.6.1.3	Se A.6.1.3
A.6.1.5	Informationssikkerhed ved projektstyring Informationssikkerhed skal anvendes ved projektstyring, uanset projekttype.	Ingen	Vi har indhentet dokumentation for, at der er etableret en formel change management-proces. Vi har med baggrund i afsluttede netværksændringer for den periode, der revideres, gennem stikprøver, testet, om	For 3 af de 15 udvalgte stikprøver var der ikke en formel testplan samt fall back strategi. Ingen yderligere bemærkninger

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
			netværksændringer har fulgt processen.	

4.3.3 A.7.1. Før ansættelse (ISO 27001)

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål: At sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til. DS/ISO IEC 27002:2014				
A.7.1.1	Screening Efterprøvning af alle jobkandidaters baggrund skal udføres i overens-stemmelse med relevante love, forskrifter og etiske regler og stå i forhold til de forretnings-mæssige krav, klassifika-tionen af den informa-tion, der gives adgang til, og de relevante risici.	Ingen	Vi har med baggrund i ansættelser for den periode, der revideres, gennem stikprøver testet, at der er indhentet sikkerhedsgodkendel ser fra hhv. Krimi-nalforsorgen og Forsvarets Efter-retningstjeneste	Ingen væsentlige bemærkninger
A.7.1.2	Ansættelsesvilkår og –betingelser Kontrakter med medarbejdere og kontrahenter skal beskrive de pågældendes og organisationens ansvar for informations-sikkerhed.	Ingen	Vi har med baggrund i ansættelser for den periode, der revideres, gennem stikprøver testet, at ansvaret for infor-mationssikkerhed fremgår af kontrak-ter, herunder tavshedspligt.	Ingen væsentlige bemærkninger

4.3.4 A.7.2. Under ansættelse (ISO 27001)

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål: At sikre, at medarbejdere og kontrahenter er bevidste og lever op til deres informationssikkerhedsansvar. DS/ISO IEC 27002:2014				

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
A.7.2.1	Ledelsesansvar Ledelsen skal kræve, at alle medarbejdere og kontrahenter opretholder informationssikkerhed i overensstemmelse med organisationens fastlagte politikker og procedurer.	Ingen	Vi har forespurgt ledelsen, om den er bevidst om sit ansvar for informationssikkerhed. Vi har endvidere med baggrund i ansættelser for den periode, der revideres, gennem stikprøver testet, at it-sikkerhedshåndbogen er udleveret i forbindelse med ansættelsen.	Ingen væsentlige bemærkninger
A.7.2.2	Bevidsthed om uddannelse og træning i informationssikkerhed Alle organisationens medarbejdere og, hvor det er relevant, kontrahenter skal ved hjælp af uddannelse og træning bevidstgøres om sikkerhed og regelmæssigt holdes ajour om organisationens politikker og procedurer, i det omfang dette er relevant for deres jobfunktion.	Ingen	Vi har med baggrund i ansættelser for den periode, der revideres, gennem stikprøver af tiltrådte medarbejdere testet, at de har underskrevet en erklæring om, at de er bekendt med it-sikkerhedspolitikken. Vi har endvidere konstateret, at der årligt foretages en awareness-øvelse. Endelig har vi påset, at it-sikkerhedspolitikken ligger på intranettet.	Ingen væsentlige bemærkninger
A.7.2.3	Sanktioner Der skal være etableret en formel og kommunikeret sanktionsproces, så der kan skrides ind over for medarbejdere, der har begået informationssikkerhedsbrud.	Ingen	Vi har indhentet sikkerhedspolitikken og konstateret, at denne beskriver forhold vedr. sanktioner	Ingen væsentlige bemærkninger

4.3.5 A.9.1 Forretningsmæssige krav til adgangsstyring (ISO 27001)

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål: At forhindre uautoriseret offentliggørelse, ændring, fjernelse eller destruktion af information lagret på medier. DS/ISO IEC 27002:2014				

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
A.9.1.1	Politik for adgangsstyring En politik for adgangsstyring skal fastlægges, dokumenteres og gennemgås på grundlag af forretnings- og informationssikkerheds-krav.	Ingen	Vi har indhentet it-sikkerhedshåndboge n og konstateret, at denne beskriver kravene til Nianets medarbejdere i relation til adgange, herunder oprettelse, identificering og adgang.	Ingen væsentlige bemærkninger
A.9.1.2	Adgang til netværk og netværkstjenester Brugere skal kun have adgang til de netværk og netværkstjenester, som de specifikt er autoriseret til at benytte.	Ingen	Vi har indhentet it-sikkerhedshåndboge n og konstateret, at denne definerer retningslinjer for anvendelsen af VPN-forbindelser og åbne netværk.	Ingen væsentlige bemærkninger.

4.3.6 A.9.2 Administration af bruger adgange (ISO 27001)

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål: At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester. DS/ISO IEC 27002:2014				
A.9.2.1	Brugerregistrering og afmelding En politik for adgangs-styring skal fastlægges, dokumenteres og gen-nemgås på grundlag af forretnings- og infor-mationssikkerhedskrav.	Ingen	Vi har indhentet dokumentation for, at der er etableret procedurer for oprettelse og nedlæggelse af brugeradgange.	Ingen væsentlige bemærkninger
A.9.2.2	Tildeling af brugeradgang Der skal implementeres en formel procedure for tildeling af brugeradgang med henblik på at tildele eller tilbagekalde ad-gangsrettigheder for alle brugertyper til alle systemer og tjenester.	Ingen	Vi har med baggrund i ansættelser for den periode, der revide-res, gennem stik-prøver testet, at tildelte adgange er formelt godkendt og har fulgt proceduren for adgangsstyring.	Ingen væsentlige bemærkninger
A.9.2.3	Styring af privilegerede adgangsrettigheder	Ingen	Vi har med baggrund i ansættelser for den periode, der revi-	Ingen væsentlige bemærkninger

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
	Tildeling og anvendelse af privilegerede adgangsrettigheder skal begrænses og styres.		deres, gennem stikprøver testet, at tildelte privilegerede adgangsrettigheder er formelt godkendt og har fulgt proceduren for adgangsstyring.	
A.9.2.4	Styring af hemmelig autentifikationsinformation om brugere Tildeling af hemmelig autentifikationsinformation skal styres ved hjælp af en formel administrationsproces.	Ingen	Vi har inspiceret, at Nianet har en formaliseret proces i relation til behandling af følsomme data. Vi har endvidere med baggrund i ansættelser for den periode, der revideres, gennem stikprøver testet, at medarbejder er blevet screenet før ansættelse.	Ingen væsentlige bemærkninger
A.9.2.5	Gennemgang af brugeradgangsrettigheder Aktivejere skal med jævne mellemrum gennemgå brugernes adgangsrettigheder.	Ingen	Vi har inspiceret proceduren for adgangsstyring, herunder retningslinjerne for periodisk gennemgang af tildelte systemadgange og rettigheder. Vi har endvidere stikprøvevist testet for den periode, der revideres, at Nianet har udført en periodisk gennemgang af tildelte systemadgange og rettigheder.	Vi har konstateret, at der ikke i revisionsperioden er gennemført en gennemgang af tildelte systemadgange og rettigheder. Ingen yderligere bemærkninger
A.9.2.6	Inddragelse eller justering af adgangsrettigheder Alle medarbejderes og eksterne brugeres adgangsrettigheder til information og informationsbehandlingsfaciliteter skal inddrages, når	Ingen	Vi har med baggrund i fratrædelser for den periode, der revideres, gennem stikprøver testet, at fratrådte medarbejdere har fået inddraget deres systemadgange.	Ingen væsentlige bemærkninger

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Testplan	Testresultat
	deres ansættelses-forhold, kontrakt eller aftale ophører eller skal tilpasses efter en ændring.			

4.3.7 A.11.1 Fysisk sikkerhed (ISO 27001)

	Kontrolaktiviteter	Kundernes overvejelser om kontroller	Testplan	Testresultat
Kontrolmål A.11.1: At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter. DS/ISO IEC 27002:2014.				
A.11.1.1	Fysisk perimetersikring Kontrol: Der skal defineres og anvendes perimetersikring til at beskytte områder, der indeholder enten følsomme eller kritiske informationer og Informationsbehand-lingsfaciliteter.	Ingen	Vi har for driftscentrene påset, at der er installeret videoovervågning, adgangskontrol, aflåste rackskabe, vand- og fugtdetek-torer samt hævede edb-gulve. Vi har endvidere for driftscentrene påset, at indretning og udformning er i overensstemmelse med sikringskrav 40S, herunder at der er installeret AIA-alarmanlæg samt adgangssluser.	Ingen væsentlige bemærkninger
A.11.1.2 Interne	Fysisk adgangskontrol (interne) Kontrol: Sikre områder skal være beskyttet med passende adgangs-kontrol for at sikre, at kun autoriseret per-sonale kan få adgang.	Ingen	Vi har med baggrund i oprettelser/ændrin-ger for den periode, der revideres, gen-nem stikprøver testet, at adgangs-tildelinger i løbet af perioden er korrekt godkendt.	Ingen væsentlige bemærkninger
A.11.1.2 Eksterne	Fysisk adgangskontrol (eksterne) Kontrol: Sikre områder skal være beskyttet med passende adgangs-kontrol for at sikre, at kun autoriseret perso-nale kan få adgang.	Ingen	Vi har med baggrund i eksterne opret-telser/ændringer for den periode, der revideres, gennem stikprøver testet, at adgangstildelinger i løbet af perioden er korrekt godkendt.	Ingen væsentlige bemærkninger

	Kontrolaktiviteter	Kundernes overvejelser om kontroller	Testplan	Testresultat
A.11.1.3	Sikring af kontorer, lokaler og faciliteter Kontrol: Fysisk sikring af kontorer, lokaler og faciliteter skal tilrettelægges og etableres.	Ingen	Vi har for drifts-centrene påset, at der er installeret videoovervågning, adgangskontrol, aflåste rackskabe, vand- og fugtdetek-torer samt hævede edb-gulve. Vi har med baggrund i eksterne oprettelser for den periode, der revideres, gennem stikprøver testet, at nøglebrikker er ble-vet korrekt godkendt og udleveret.	Ingen væsentlige bemærkninger
A.11.1.4	Beskyttelse mod eksterne og miljø-mæssige trusler Kontrol: Fysisk beskyt-telse mod naturkata-strofer, ondsindede angreb eller ulykker skal tilrettelægges og etableres.	Ingen	Vi har for drifts-centrene påset, at der er installeret: 1) redundant UPS- og dieselgeneratorer. 2) brandsluknings-anlæg samt brand- og røgalarmer. 3) klimaanlæg samt CTS-system til auto-matisk klimaover-vågning, og påset, at CTS-systemet automatisk opretter alarmer i NOC'en. Endvidere har vi kontrolleret, om der er foretaget periodisk serviceeftersyn af UPS og dieselgenera-torerne, brandsluk-ningsanlæggene og klimanlæggene.	Ingen væsentlige bemærkninger
A.11.1.5	Arbejde i sikre områder Kontrol: Procedurer for arbejde i sikre områder skal tilrettelægges og etableres.	Ingen	Vi har konstateret, at der er udarbejdet retningslinjer for adgang til Nianets datacenter, og stikprøvevist påset, at når der er tildelt en adgang til	Ingen væsentlige bemærkninger.

	Kontrolaktiviteter	Kundernes overvejelser om kontroller	Testplan	Testresultat
			datacentrene, har vedkommende kvitteret for at have læst retningslinjerne for adgang til Nianets datacentre.	
A.11.1.6	Områder til af- og pålæsning Kontrol: Adgangssteder som fx områder til af- og pålæsning og andre steder, hvor uautori-serede personer kan komme ind på området, skal styres og så vidt muligt adskilles fra informationsbehandlings-faciliteter for at undgå uautoriseret adgang.	Ingen	Vi har for drifts-centrene påset, at områder til af- og pålæsning er adskilt fra driftscentrene. Vi har endvidere påset, at der er installeret AIA-alarmanlæg samt adgangssluser.	Ingen væsentlige bemærkninger