Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C
Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

Nianet A/S

ISAE 3000-erklæring fra uafhængig revisor vedr. udvalgte kontroller relateret til Lov om net- og informationssikkerhed for perioden 16. juni 2017 til 7. juni 2018

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56
Weidekampsgade 6
Postboks 1600
0900 København C
Telefon 36 10 20 30
Telefax 36 10 20 40
www.deloitte.dk

Nianet A/S
Att.: Christian Holm Christensen
Ejby Industrivej 1
2600 Glostrup

Erklæring fra uafhængig revisor vedr. forhold relateret til Lov om net- og informationssikkerhed

Indledning

Nianet er et it-driftsselskab med fokus på datakommunikationsløsninger baseret på fiber til offentlige og private erhvervsvirksomheder. Nianet er landsdækkende og ejer fiber til mere end 4.000 unikke adresser.

Som en væsentlig udbyder af datakommunikationsløsninger i Danmark er Nianet underlagt bekendtgørelse om beredskabsaktørers adgang til elektronisk kommunikation nr. 564 af 1. juni 2016, bekendtgørelse om sikkerhedsgodkendelse af medarbejdere på net- og informationssikkerhedsområdet nr. 565 af 1. juni 2016, bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed nr. 566 af 1. juni 2016 og bekendtgørelse om informationssikkerhed og beredskab i net og tjenester nr. 567 af 1. juni 2016 i Lov om net- og informationssikkerhed fra Forsvarsministeriet (herefter NIS-loven). Nianets ledelse har beskrevet de væsentligste politikker og procedurer, som ledelsen finder relevante i forhold til overholdelse af bekendtgørelsernes krav i Bilag 1 samt de kontrolmål og kontroller, som ledelsen vurderer relevante i tilknytning hertil i Bilag 2.

Erklæringen omfatter gennemgang af, hvorvidt den af ledelsen udarbejdede systembeskrivelse i Bilag 1 samt de i Bilag 2 beskrevne kontroller er retvisende i forhold til de faktisk implementerede kontroller og procedurer, samt hvorvidt disse har fungeret i perioden fra d. 16. juni 2017 til d. 7. juni 2018.

Denne erklæring omfatter ikke kontroller relateret til underleverandører.

Ledelsens ansvar

Det er ledelsens ansvar at identificere relevante kontrolmål til afdækning af relevante sikkerhedskrav og sikre, at de relevante kontroller, der understøtter overholdelse af kravene i NIS-loven, var hensigtsmæssigt udformet og implementeret i perioden fra d. 16. juni 2017 til d. 7. juni 2018.

Revisors ansvar og den udførte gennemgang

Det er vores ansvar, baseret på vores procedurer, at udtrykke en konklusion om Nianets beskrivelse, og hvorvidt vi er enige i, at de af ledelsen etablerede kontroller til overholdelse af kravene i NIS-loven var hensigtsmæssigt udformet og implementeret i perioden fra d. 16. juni 2017 til d. 7. juni 2018.

De kriterier, som vi har lagt til grund for vores vurdering af, hvorvidt de udvalgte kontroller, der knytter sig til de af ledelsen identificerede kontrolmål, i alle væsentlige henseender var hensigtsmæssigt udformet og implementeret i perioden fra d. 16. juni 2017 til d. 7. juni 2018, er som følger:

a) De risici, som truede overholdelsen af de kontrolmål, der er anført i bilag 2, var identificeret af ledelsen.
b) De af ledelsen identificerede kontroller ville, hvis anvendt som beskrevet, give en høj grad af sikkerhed for, at de pågældende risici ikke ville forhindre opnåelsen af de anførte kontrolmål.

Vores arbejde er udført i overensstemmelse med revisionsstandard ISAE 3000, således at der opnås en høj, men ikke fuldstændig grad af sikkerhed for vores konklusioner. En erklæringsopgave med sikkerhed om at afgive erklæring om udformningen og funktionaliteten af kontroller hos en serviceleverandør omfatter udførelse af handlinger for at opnå bevis for oplysningerne i serviceleverandørens beskrivelse af sit system samt for kontrollernes udformning og funktionalitet. De valgte handlinger afhænger af serviceleverandørens revisors vurdering, herunder vurderingen af risiciene for, at kontrollerne ikke er hensigtsmæssigt udformet eller ikke fungerer effektivt. Vores handlinger har omfattet test af funktionaliteten af sådanne kontroller, som vi anser for nødvendige for at give høj grad af sikkerhed for, at de udvalgte kontroller, der knytter sig til de af ledelsen identificerede kontrolmål, blev nået.

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 til kvalitetsstyring, herunder dokumenterede politikker og procedurer for overholdelse af etiske regler, faglige standarder samt gældende krav i lov og øvrig regulering.

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

Konklusion

Vores konklusion er udformet på grundlag af de forhold, der er redegjort for i denne erklæring. De kriterier, som vi har anvendt ved udformningen af konklusionen, er de kriterier, som er anført i ovenstående. På grundlag af det udførte arbejde er det vores opfattelse, at den af Nianet udarbejdede systembeskrivelse i bilag 1 med tilhørende beskrivelse af relaterede kontrolmål og kontroller i bilag 2 i det væsentligste er retvisende i forhold til de faktisk etablerede procedurer og kontroller, og at disse har været implementeret og har fungeret effektivt i perioden fra d. 16. juni 2017 til d. 7. juni 2018.

København, den 27.06.2018

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR-nr. 33 96 35 56

Thomas Kühn
statsautoriseret revisor

Jesper Due Sørensen
partner, CISA

Bilag 1 Systembeskrivelse fra Nianet

Introduktion

Denne beskrivelse er udfærdiget med det formål at give information omkring de kontroller, der anvendes i forhold til levering af datakommunikationsløsninger samt omkring de kontroller, der anvendes relateret til NIS-loven.

Omfang

Beskrivelsen omfatter de ydelser, der leveres af Nianet, og fokuserer på kontrolmål, der er relevante for de interne kontroller, som relaterer sig til NIS-loven og specifikke yderligere kontraktuelt aftalte kontroller for Nianets kunder. Beskrivelsen omfatter de forretningsprocesser og kontrolmål, som Nianet har fastslået som væsentlige for deres kunder ud fra et informationssikkerhedsmæssigt synspunkt. Ledelsen i Nianet er ansvarlig for identifikation af kontrolmål og for 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 fælles standardiserede processer. Specifikke kontroller i forbindelse med krav i EU persondataforordning (GDPR) er som udgangspunkt 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 4.000 unikke adresser via mange tusind kilometer fiber. Nianet blev etableret i maj 2003 og er til d. 8. juni 2018 ejet af 13 danske energiselskaber fordelt over hele landet. Pr. 8. juni 2018 er Nianet solgt til GlobalConnect A/S, Hørskætten 3-5, 2630 Taastrup.

It-services

Nianet leverer datakommunikationsløsninger, co-location samt cloudløsninger.

Ydelserne inkluderer bl.a.:

- MPLS VPN
- Internettrafik
- Managed LAN
- Sort og grå fiber
- DSL-forbindelser
- Internationale forbindelser
- Co-location/housing
- Private Cloud, Virtuel Server og flere typer backup-løsninger bl.a. Backup as a Service (BaaS)
- Hosted firewall og selfmanaged Firewall
- Anti-DDoS-løsninger
- Hardware og Software VPN.

Systembeskrivelsen omfatter kontrolaspekter, som relaterer sig til informationssikkerhed, risikostyring og beredskab og sigter mod efterlevelse af NIS-loven m.v.

Rammeværk

System- og kontrolbeskrivelsen er baseret på den internationale informationssikkerhedsstandard ISO/IEC 27001, Lov om net- og informationssikkerhed og de fire bekendtgørelser, som regulerer NIS-loven, samt endelig forretningsmæssige krav i de ydelser, der tilbydes af Nianet, herunder:

- Fysisk og logisk sikring
- Risikostyring
- Beredskab.

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, processer, procedurer, metoder og organisatorisk struktur. Følgende beskriver Nianets kontrolmiljø, og Nianets leverancer af it-services:

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

Ansvar, Nianets bestyrelse og direktion

Nianet ejes indtil d. 8. juni 2018 af 13 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 overholdelse af Nianets politikker – herunder informationssikkerhedspolitikken. 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 150 medarbejdere.

Nianets direktion ser ud som følger:

- Administrerende direktør – Rasmus Helmich
- Økonomidirektør – Søren Fæster Nielsen
- Salgs- og marketingdirektør – Peter Sandahl Torp
- Leverancedirektør - Mette Slesvig
- Teknisk direktør – Per Skovgaard Rosen.

Pr. den 8. juni 2018 overgår ejerskab af Nianet til GlobalConnect, og der er fra denne dato indsat en bestyrelse og direktion bestående af:

- Bestyrelsesformand Pernille Ravn
- Menigt bestyrelsesmedlem Mikkel Bønnelycke
- Menigt bestyrelsesmedlem Kent Vinhardt Josephsen
- Menigt bestyrelsesmedlem Christian Holm Christensen
- Menigt bestyrelsesmedlem Thomas Caspersen Nielsen

- Medarbejdervalgt medlem Karsten Lykke Høvdinghoff
- Medarbejdervalgt medlem Carsten Jørgensen
- Medarbejdervalgt medlem Martin Hein Lippert
- Medarbejdervalgt medlem Søren Kristensen
- Medarbejdervalgt medlem Thomas Guvad (suppleant)
- Medarbejdervalgt medlem Iben Nielsen (suppleant)
- Medarbejdervalgt medlem Morten Dejgaard Birkelund (suppleant)
- Administrerende direktør Christian Holm Christensen

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

Risikostyring

Risikovurdering

Ledelsen mødes regelmæssigt for at diskutere 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, baseret på ISO/IEC 27005. Den anvendte model til vurdering af risici omfatter en vurdering af konsekvens, sandsynlighed, sårbarhed og etablerede foranstaltninger. Processen tager både eksterne og interne faktorer og trusler i betragtning tillige med ledelsens evne til at fokusere på disse faktorers påvirkning af driften.

Risikoanalysen indeholder ledelsesvurdering og håndtering af risiko.

It-sikkerhedspolitik og sikringsplaner

Der er på baggrund af risikovurdering og sårbarhedsanalyse udarbejdet it-sikkerhedspolitik, sikringsplaner, processer og procedurer, der har til formål at imødegå identificerede risici.

Nianets sikringsplaner inkluderer planer til at sikre, at særligt kritiske dele af virksomhedens administrative systemer, infrastruktur herunder datacentre og større POPs (Point-Of-Presence) har en lav sårbarhed. Sikringsplanerne testes og vedligeholdes i henhold til en fastlagt og godkendt testplan. It-sikkerhedspolitik, sikringsplaner, processer og procedurer revurderes årligt i sammenhæng med den årlige risikovurdering samt under hensyntagen til resultaterne af udførte tests.

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 underskrive aftalen.

Overvågning og kommunikation

Nianet overvåger og registrerer brud på it-sikkerhed samt persondatasikkerhed gennem en formelt dokumenteret incident management-proces. Alle incidents registreres og dokumenteres i et sagsstyringssystem. Registrering og dokumentation for incidents gemmes i systemet.

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 og Nianets direktion.

Påbud og informationer fra offentlige myndigheder og styrelser overvåges af Nianets kontaktpunkt til offentlige myndigheder samt af CTO.

Beredskab

Beredskabs- og kriseplaner

Nianet har på baggrund af årligt udførte risikovurderinger udarbejdet og implementeret beredskabspolitik og beredskabsplaner til efterlevelse af BEK 564 og 567. Beredskabsplaner og politik indeholder sikring af alle områder specificeret i bekendtgørelser og i den udarbejdede risikovurdering. Nianet har udarbejdet beredskabsplaner for fysisk skade på alle væsentlige lokationer og en krisehåndteringsplan, der er fælles for alle større incidents, 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 sammen med revurdering af beredskabsplaner.

Sikkerhed

Der foreligger politikker, procesbeskrivelser, procedurer og arbejds- og kontrolbeskrivelser af væsentlige og kritiske områder vedrørende fysisk og logisk sikkerhed.

Sikkerhed, fysisk adgang

Nianet A/S har implementeret formelle politikker, procesbeskrivelser og procedurer med henblik på adgangskontrol til systemer, faciliteter og datacentre. Disse politikker mv. definerer de niveauer af adgang, der er tilladt iht. klassifikation af medarbejdere og beskriver de tiltag og tilladelser, der er krævet i forhold til at opnå og overvåge adgang.

Administration af adgangskontrol

Datacenterindgange er sikret af elektroniske læsere af adgangskort, som er forbundet med et centralt ADK-system. Adgang til datacentre administreres ud fra arbejdsopgaver og klassifikation af Nianets Network Operations Center (NOC). Det kræves, at kunden giver detaljer om det niveau af adgange, der rekvireres, tillige med behørig tilladelse, før adgangskort udarbejdes og udleveres. Der udstedes personlige adgangskort med tilhørende personlig, hemmelig adgangskode. Kunder med adgang til datacentre har udelukkende adgang til eget aflåst rackskab eller område.

Overvågning

Adgange til datacentre er udstyret med alarmer og overvåges med videokameraer. Videoaktivitet overføres til et centralt CCTV-system. Sikkerhedspersonale 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, forsynet med eskorte.

Fysiske sikringsforanstaltninger

Datacentre er opført i henhold til Uptime Tier2- eller Tier3-definition. Datacentre er forsynet fra den lokale eldistributør og gennem standby-generatorer og via 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 elleverance. Generatorerne og UPS-anlæg m.v. testes regelmæssigt i henhold til årshjul – 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 omgivende rum, hvorfra et køleaggregat suger 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 %.

Områder, der benyttes til placering af 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 kontrolcentral.

Området er videoovervåget, og al aktivitet logges.

Datacentre er S40-certificerede.

Brugerkontrol – hensyn til kunder

Nianets kontroller er designet ud fra den antagelse, at visse interne kontroller er implementeret hos kunderne/brugerne. Implementeringen af sådanne interne kontroller er nødvendige for at opnå de kontrolmål, som er beskrevet i sektion 4. Der kan være yderligere kontrolmål og relaterede kontroller hos kunderne/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. Kontrolovervejelser, som er anført nedenfor, skal ikke ses som en fyldestgørende liste over 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.

Bilag 2 Kontrolmål, kontroller og udførte testhandlinger

Nedenfor vises resultatet af vores testhandlinger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
Kontrolmål: At give retningslinjer for og understøtte beredskabsaktørers adgang til elektronisk kommunikation i beredskabssituationer. Bek 564.				
B1_001	*Faste kredsløb – proces.* Nianet har i deres beredskabsproces registreret og prioriteret faste kredsløb til beredskabsmæssige formål, der er bestilt af offentlige og private kunder i henhold til BEK 564 § 10 og 11.	Ingen	Vi har inspiceret netværksmonitoreringssystemet og påset, at systemet indeholder detaljer om linjers ID, kapacitet og nettermineringspunkter. Endvidere er det påset, at der er udarbejdet en VIP-liste, som angiver de mest vitale og højest prioriterede kredsløb.	Ingen væsentlige bemærkninger.
B1_002	*Faste kredsløb– registrering*. Nianet opretholder et register med kredsløb til beredskabsmæssige formål. Registeret indeholder information om: 1) at registrere kredsløbet med et entydigt identifikationsnummer, 2) at registrere de kredsløb, som bestiller angiver som vitale kredsløb, med højeste omlægningsprioritet 3) at registrere kredsløbets transmissionskapacitet og nettermineringspunkter 4) forud for arbejdets udførelse at tage kontakt til den kontaktperson hos bestilleren, der er angivet i bestillingen, med henblik på tilrettelæggelse af arbejdets udførelse 5) at underrette bestiller, hvis bestillingen ikke kan udføres som anført i bestillingen. Udbyderen har pligt til at registrere efterfølgende nedkobling af faste kredsløb til beredskabsmæssige formål. Udbyderen skal sikre, at kredsløb, hvor mindst et nettermineringspunkt er placeret i udlandet, kan identificeres ved det identifikationsnummer, som bestiller angiver. I henhold til BEK 564 § 11.	Ingen	1) Vi har inspiceret for udvalgte stikprøver, at kredsløb er registreret med unik identifikationsnummer. 2) Vi har inspiceret, at vitale kredsløb er registreret med højeste omlægningsprioritet. 3) Vi har inspiceret for udvalgte stikprøver, at nettermineringspunkter samt transmissionskapacitet er registreret. 4 og 5) Vi har inspiceret, at Nianet har fastlagt procedurer for at tage kontakt til kontaktperson hos bestiller forud for arbejdets udførelse samt for underretning af bestiller, hvis arbejdet ikke kan udføres.	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
B1_003	*Faste kredsløb– prioritering.* Nianet har i deres beredskabsproces prioriteret de faste kredsløb til beredskabsmæssige formål, således at Nianet først foretager retablering af de faste kredsløb til beredskabsmæssige formål, som er registreret som vitale kredsløb, og derefter foretager retablering af øvrige faste kredsløb til beredskabsmæssige formål. Retableringen af de faste kredsløb til beredskabsmæssige formål skal ske forud for øvrige retableringer. I henhold til BEK 564 § 14	Ingen	Se B1_002	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
Kontrolmål: At Sikre, at medarbejdere og kontrahenter forstår deres ansvar og er egnede til de roller, de er i betragtning til vedrørende net- og informationssikkerhed. Bek 565				
B2_001	*It-sikkerhedsledelse – medarbejdere.* Alle medarbejdere med adgang til kundeklassificerede informationer er sikkerhedsgodkendt til klassifikationsgraden HEMMELIGT i overensstemmelse med Justitsministeriets cirkulære om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU.	Ingen	Vi har inspiceret for udvalgte stikprøver, at medarbejdere med adgang til kundeklassificerede informationer er sikkerhedsgodkendt til klassifikationsgraden HEMMELIGT.	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
Kontrolmål: At give retningslinjer for og understøtte oplysnings- og underretningspligter vedrørende net- og informationssikkerhed. Bek 566				
B3_001	*Underretningspligt – aftaleindgåelser* Nianet har fastlagt procedurer for skriftligt at underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger om aftaler samt tillæg til eksisterende aftaler, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf i henhold til BEK 566 § 3 og § 4. Underretninger skal indeholde oplysninger om: 1) Hvilke kritiske netkomponenter, systemer og værktøjer, herunder varetagelse af driften heraf, som aftalen påtænkes at omfatte 2) Aftalens påtænkte omfang 3) Eventuel placering af opgaver uden for Danmark 4) Eventuelle leverandører, der påtænkes inddraget i aftaleforhandlingerne 5) Overordnet tidsplan for aftaleforhandlingerne 6) Aftalens påtænkte varighed.	Ingen	Vi har inspiceret procedurer for rapportering til Center for Cybersikkerhed forud for, at der indledes forhandlinger om aftaler samt tillæg til eksisterende aftaler, der vedrører kritiske netkomponenter i henhold til BEK 566 § 3 og § 4.	Vi har fået oplyst, at der ikke har været tilfælde, som har nødvendiggjort forhandlinger af den omtale karakter. Ingen yderligere bemærkninger
B3_002	*Underretningspligt – underretning* Nianet har i incident management-proces fastlagt procedurer for rapportering af hændelser til Center for Cybersikkerhed vedr. brud på informationssikkerheden i henhold til BEK 566 § 7 og 8.	Ingen	Vi har inspiceret dokumentation for, at der i forlængelse af Nianets incident management-proces er oprettet procedurer for rapportering af hændelser til Center for Cybersikkerhed.	Ingen væsentlige bemærkninger.
B3_003	*Underretningspligt – kunder* Nianet har indhentet oplysninger fra tjenesteudbydere, der benytter udbydernes net, med henblik på at kunne foretage underretning i henhold til BEK 566 § 9 og § 10.	Ingen	Vi har inspiceret incident management-proceduren for håndtering af nedbrud, samt hvordan incidents skal eskaleres. Vi har påset, at kontaktoplysninger på tjenesteudbydere er nedskrevet i oversigtsark i relation til underretning i henhold til BEK 566 § 9 og § 10.	Ingen væsentlige bemærkninger.
B3_004	*Underretningspligt – Kontaktpunkt* Der er indberettet kontaktpunkt til projektenheden for cybersikkerhed.	Ingen	Vi har inspiceret dokumentation for, at der er indberettet kontaktpunkt til projektenheden for cybersikkerhed.	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
Kontrolmål: At give retningslinjer for og understøtte informationssikkerhed og beredskab i net og tjenester. BEK 567				
B4_001	*It-sikkerhedsledelse – it-risikoanalyse.* Der er udarbejdet it-risikoanalyse efter anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende, som tager stilling til risikoen for tab af tilgængelighed, integritet og fortrolighed i de net og tjenester, der udbydes, samt efterlever krav i BEK 567 § 2 og § 5. Risikovurderingen skal inkludere tredjeparter (samarbejdspartner). Risikoanalyse revurderes årligt samt ved væsentlige ændringer.	Ingen	Vi har indhentet seneste it-risikoanalyse og kontrolleret, at denne er godkendt og udarbejdet efter ISO 27005. Vi har endvidere kontrolleret, at der er udarbejdet en risikovurdering, der inkluderer tredjeparter.	Ingen væsentlige bemærkninger.
B4_002	*It-sikkerhedsledelse – ledelsessystem til risikostyring.* Der er udarbejdet et formelt ledelsessystem til samlet risikostyring af informationssikkerhed. Der skal i den forbindelse tages stilling til kriterier for Nianets risikovillighed med henblik på at opretholde net og tjenester i beredskabssituationer. I henhold til BEK 567 § 6 og 7.	Ingen	Vi har inspiceret dokumentation med henblik på at kontrollere, at der er udarbejdet et formelt ledelsessystem efter ISO 27005 til samlet risikostyring af informationssikkerhed, som tager stilling til kriterier for Nianets risikovillighed i henhold til BEK 567 § 6 og 7.	Ingen væsentlige bemærkninger.
B4_003	*It-sikkerhedsledelse – informationssikkerhedspolitikken* Der er på baggrund af en it-risikoanalyse udarbejdet en informationssikkerhedspolitik med udgangspunkt i en anerkendt international standard, eksempelvis DS/ISO/IEC 27001 eller tilsvarende, for at imødegå identificerede risici. Informationssikkerhedspolitikken revurderes årligt samt ved væsentlige ændringer. Informationssikkerhedspolitikken skal efter § 3 desuden beskrive udbydernes politik for håndtering af beredskabssituationer og andre ekstraordinære situationer med henblik på at sikre, at net og tjenester i videst muligt omfang kan opretholdes i sådanne situationer. I henhold til BEK 567 § 7.	Ingen	Vi har inspiceret gældende informationssikkerhedspolitik og kontrolleret, at denne er udarbejdet efter ISO 27001-standarden. Vi har påset, at politikken er revurderet og godkendt i erklæringsperioden samt at denne omhandler håndtering af beredskabssituationer i henhold til BEK 567 § 7.	Ingen væsentlige bemærkninger.
B4_004	*It-sikkerhedsledelse – awareness* Alle medarbejdere hos Nianet skal kvittere for at have læst informationssikkerhedspolitikken og trusselsbilledet/risikovurderingen i henhold til BEK 567 § 10.	Ingen	Vi har med baggrund i tiltrædelser for erklæringsperioden stikprøvevist kontrolleret, at medarbejderne hos Nianet har kvitteret for at have læst informationssikkerhedspolitikken i henhold til BEK 567 § 10.	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
B4_005	*It-sikkerhedsledelse – informationssikkerhedsorganisation.* It-sikkerhedsrelevante opgaver er formelt defineret, og ansvaret for opgaverne er placeret hos medarbejdere, som er bekendte med deres ansvar i henhold til BEK 567 § 8 og 15.	Ingen	Vi har inspiceret gældende informationssikkerhedspolitik og kontrolleret, at denne beskriver it-sikkerhedsorganisationen samt indeholder en beskrivelse af de forskellige rollers ansvar.	Ingen væsentlige bemærkninger.
B5_006	*It-sikkerhedsledelse – it-beredskab* Der er på baggrund af it-risikoanalysen og informationssikkerhedspolitikken udarbejdet beredskabsplaner til håndtering af beredskabssituationer. Beredskabsplanerne skal med udgangspunkt i Nianets risikovillighed tage højde for, at Nianet kan opretholde udbuddet af net og tjenester i beredskabssituationer og i andre ekstraordinære situationer. Beredskabsplaner revurderes årligt. I henhold til BEK 567 § 7.	Ingen	Vi har inspiceret, at Nianet har etableret en beredskabsplan, som tager afsæt i risikoanalysen. Vi har kontrolleret, at beredskabsplanen tager højde for, at Nianet kan opretholde udbuddet af net og tjenester i beredskabssituationer og i andre ekstraordinære situationer.	Ingen væsentlige bemærkninger.
B5_007	*It-sikkerhedsledelse – it-beredskabstest og øvelser* Der er udarbejdet en flerårig rotationsplan for beredskabsøvelser.	Ingen	Vi har inspiceret den femårige testplan for beredskabsøvelser samt indhentet dokumentation på udført beredskabstest i erklæringsperioden.	Ingen væsentlige bemærkninger.
B5_008	*It-sikkerhedsledelse – register over kritiske netkomponenter, systemer og værktøjer.* Nianet har til brug for risikostyringen etableret et register over kritiske netkomponenter, systemer og værktøjer. Registret vedligeholdes og opdateres ved ændringer i henhold til BEK 567 § 11.	Ingen	Se kontrol B1_001.	Ingen væsentlige bemærkninger.
B5_009	*It-sikkerhedsledelse – it-sikringsplaner* Der er på baggrund af it-risikoanalysen udarbejdet sikringsplaner for at imødegå identificerede risici. Sikringsplanen skal som minimum tage stilling til logisk og fysisk adgangskontrol, fysisk perimetersikring, brandsikring, klimasikring samt varslingssystemer til detektion af uautoriseret adgang. Sikringsplaner revurderes årligt.	Ingen	Vi har indhentet kopi af seneste sikringsplaner og vurderet: • Om der er formel godkendelse på et tilstrækkeligt ledelsesniveau • Om den er udarbejdet på baggrund af en it-risikoanalyse • Om ansvaret for implementeringen af politikken er klart placeret • Om sikringsplanerne tager stilling til logisk og fysisk adgangskontrol samt fysisk perimetersikring.	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
B5_010	*It-sikkerhedsledelse – systemlogning* Nianet har etableret procedure for at implementere logning med henblik på at sikre sporbarhed ved eventuelle informationssikkerhedsbrud, herunder at administratorrettigheder logges i henhold til BEK 567 § 13. Nianet har endvidere en kontrol for periodisk gennemgang af logfiler.	Ingen	Vi har inspiceret gældende logpolitik samt kontrolleret, at denne efterleves på netværket og Windows-domænet. Vi har inspiceret, om logfiler gennemgås periodisk.	Vi har konstateret, at logfiler ikke er gennemgået, men opbevares med henblik på at kunne udføre en reaktiv kontrol. Ingen yderligere bemærkninger.
B5_011	*Adgang til logfiler er restriktivt opsat* Brugere med adgang til logfiler har et arbejdsbetinget behov herfor.	Ingen	Vi har stikprøvevist inspiceret, om brugere med adgang til logfiler har et arbejdsbetinget behov herfor.	Ingen væsentlige bemærkninger.
B5_012	*Adgang til logfiler igennem backup* Adgangen til logfiler igennem backup foregår via krypterede og sikrede forbindelser.	Ingen	Vi har inspiceret, at logfiler gemmes i Veaam-backupløsning på eget interne drev. Vi har endvidere inspiceret brugerlisten med MDA accounts, som har adgang til logfiler i Veaam.	Ingen væsentlige bemærkninger.
B5_013	*Netværksændringer – test* Nianet har en formel change management-proces, hvorunder det sikres, at der i forbindelse med alle ændringer til idriftsættelser sker dokumentation af den gennemførte tests omfang og kvalitet, samt at godkendelser af ændringer dokumenteres konsistent i henhold til BEK 567 § 14.	Ingen	Vi har inspiceret den formelle change management-proces og kontrolleret, at der i denne stilles krav til, at der i forbindelse med alle ændringer til idriftsættelser sker dokumentation af den gennemførte tests omfang og kvalitet, samt at godkendelser af ændringer dokumenteres konsistent i henhold til BEK 567 § 14. Vi har endvidere stikprøvevist kontrolleret, om netværksændringer har fulgt processen.	For en ud af de 25 udvalgte stikprøver var der ikke en formel godkendelse. For en ud af de 25 udvalgte stikprøver forelå der ikke fallback- og testplan. Ingen yderligere bemærkninger.
B5_014	*It-sikkerhedsledelse – sikkerhedshændelser/incident management* Særlige risici for brud på informationssikkerheden håndteres gennem incident management-proces og rapporteres igennem denne til kunden i henhold til BEK 567 § 15.	Ingen	Vi har inspiceret proceduren for behandling af risici for brud på informationssikkerheden. Vi har endvidere inspiceret populationen af incidents og kontrolleret, at der ikke har været nogen med særlige risici for brud på informationssikkerheden i revisionsperioden.	Vi har konstateret, at der ikke har været særlige risici for brud på informationssikkerheden, som har skullet håndteres igennem incident management-processen og rapporteres igennem denne til kunden.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
				Ingen yderligere bemærkninger.
B5_015	*It-sikkerhedsledelse – sårbarhedsscanning* Nianet skal til enhver tid holde sig orienteret om nye sårbarheder, der vil kunne have konsekvenser for udbydernes net og tjenester. Nianet foretager årlige sårbarhedsscanninger med henblik på at sikre, at de etablerede informationssikkerhedsforanstaltninger i net og tjenester fortsat er effektive i henhold til BEK 567 § 16.	Ingen	Vi har inspiceret dokumentation for, at Nianet i revisionsperioden har gennemført en sårbarhedsscanning af netværket.	Ingen væsentlige bemærkninger.
B5_016	*Backup – strategi* Nianet har udarbejdet en overordnet, ledelsesgodkendt backupstrategi, som danner grundlag for etableringen af backup for de relevante systemer i henhold til BEK 567 § 17.	Ingen	Vi har inspiceret ledelsesgodkendt backupstrategi og kontrolleret, at denne danner grundlag for etableringen af backup for de relevante systemer i henhold til BEK 567 § 17.	Ingen væsentlige bemærkninger.
B5_017	*Backup – test* Nianet foretager en periodisk kontrol af, at der er gennemført tilstrækkelige og tilfredsstillende retableringer af data til at underbygge formodningen om, at backupløsningen understøtter ledelses- og lovkrav i henhold til BEK 567 § 17.	Ingen	Vi har inspiceret backup- og restore-procedure og stikprøvevist kontrolleret, at der er gennemført tilstrækkelige og tilfredsstillende retableringer af data.	Ingen væsentlige bemærkninger.
B5_018	*Backup – opbevaring* Nianet har en procedure for forsvarlig og sikker opbevaring af backupmedier. F.eks. som led i en daglig checkliste. Det dokumenteres, når backupmedier bringes til den sikre opbevaring i henhold til BEK 567 § 17.	Ingen	Vi har inspiceret procedurer for forsvarlig og sikker opbevaring af backupmedier.	Ingen væsentlige bemærkninger.
B5_019	*Backup – sikker destruktion* Nianet har en procedure for sikker destruktion af backupmedier i henhold til BEK 567 § 16.	Ingen	Vi har inspiceret procedurer for forsvarlig og sikker destruktion af backupmedier.	Vi har fået oplyst, at Nianet ikke har haft backupdeske, som skulle destrueres, i revisionsperioden. Ingen yderligere bemærk-

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
				ninger.
B5_020	*Logisk adskillelse mellem miljøer* Der er logisk adskillelse mellem produktions-, administrations-, styrings- og testnet i henhold til BEK 567 § 18.	Ingen	Vi har inspiceret topologikort og kontrolleret den logiske adskillelse mellem produktions-, administrations-, styrings- og testnet.	Ingen væsentlige bemærkninger.
B5_021	*Environmental mechanisms– strømsikring* Baseret på en risikovurdering er der etableret nødstrømsløsninger (UPS og generator), som årligt serviceres og testes regelmæssigt, samt at der etableres dokumentation herfor i henhold til BEK 567 § 18.	Ingen	Vi har inspiceret driftscentrene (Skanderborg, Århus, Vallensbæk, Taastrup, Glostrup og Glostrup, Sydvestvej) og påset, at der er installeret UPS og dieselgenerator samt køle- og brandslukningsanlæg. Vi har påset servicekontrakterne for disse samt at der er gennemført service inden for erklæringsperioden.	Ingen væsentlige bemærkninger.
B5_022	*Change – informationssikkerhed* I forbindelse med en ændring til netkomponenter (anskaffelse, udvikling, ændring og vedligeholdelse) skal der ske en risikovurdering af, om ændringen kan have indvirkning på informationssikkerhed i henhold til BEK 567 § 20.	Ingen	Se B5_013	Se B5_013

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
B5_023	*Overvågning af leverandør* Nianet skal som væsentlig erhvervsmæssig leverandør sikre, at evt. samarbejdspartnere efterlever samme krav som Nianet i henhold til BEK 567 § 21 for de dele af net og tjenester, som er omfattet af samarbejdsaftaler. § 22. Såfremt der etableres et samarbejde mellem en væsentlig erhvervsmæssig udbyder af offentligt tilgængelige net og tjenester og en leverandør, er den væsentlige erhvervsmæssige udbyder af offentligt tilgængelige net og tjenester fortsat ansvarlig for, at kravene efter denne bekendtgørelse efterleves. Stk. 2. Aftaleparternes aftalegrundlag skal tage højde for informationssikkerhedsaspekter i forhold til udbuddet af net og tjenester ved samarbejdet. Aftalegrundlaget skal i fornødent omfang opdateres, hvis der sker ændringer af informationssikkerhedsmæssig betydning. Stk. 3. Udbyderen skal på baggrund af risikovurderingen efter § 2 i fornødent omfang foretage verifikation af, at der er overensstemmelse mellem aftalepartens leverancer, herunder konfigurationen af leverancerne, og det mellem parterne aftalte. Stk. 4. Verifikationen efter stk. 3 kan ske som en stikprøvekontrol, såfremt det står i forhold til udbyderens risikovurdering efter § 2.	Ingen	Vi har på baggrund af de anvendte leverandører for den periode, der revideres, stikprøvevist kontrolleret, at der foreligger underskrevet aftale vedrørende efterlevelse af BEK 567 § 21.	Ingen væsentlige bemærkninger.
B5_024	*Revision af leverandør* Ved etablering at et samarbejde efter § 21 og 22 skal de deltagende udbydere sikre, at der sker intern auditering af efterlevelsen af de informationssikkerhedskrav, der fremgår af aftalegrundlaget i henhold til BEK 567 § 23.	Ingen	Se B5_023	Se B5_023
B5_025	*Beredskabsstyring – Krisehåndteringsplaner* Der er med baggrund i risikoanalysen udarbejdet krisehåndteringsplan i henhold til BEK 567 § 27, 28 og 30.	Ingen	Vi har inspiceret gældende krisehåndteringsplan og kontrolleret, at der er udarbejdet en plan for relevante områder i henhold til BEK 567 § 27, 28 og 30.	Ingen væsentlige bemærkninger.
B5_026	*Beredskabsstyring – 24/7 vagt* Der haves en 24/7 vagtordning for beredskabssituationer i henhold til BEK 567 § 31.	Ingen	Vi har inspiceret, at Nianet har etableret en 24/7 vagtordning for beredskabssituationer.	Ingen væsentlige bemærkninger.

	Kontrolaktivitet	Kundernes overvejelser om kontroller	Udførte testhandlinger	Testresultat
B5_027	*Beredskabsstyring – underretning til Center for Cybersikkerhed* Der haves retningslinjer for straksunderretning til Center for Cybersikkerhed ved aktivering og deaktivering af beredskab i henhold til BEK 567 § 32 og § 35 samt retningslinjer for løbende (hver 4. time) situationsrapportering til Center for Cybersikkerhed i tilfælde af aktiveret beredskab i henhold til BEK 567 § 33.	Ingen	Vi har inspiceret procedurer for 'Regler for underretning om brud på informationssikkerhed - NIS lov, herunder påset, at der heri er kontaktoplysninger til Center for Cybersikkerhed.	Ingen væsentlige bemærkninger.
B5_028	*Påbud fra Center for Cybersikkerhed* Nianet skal sikre sig, at de efterlever evt. påbud fra Center for Cybersikkerhed BEK 567 § 25 og 26.	Ingen	Vi har forhørt os om, hvorvidt Nianet er underlagt evt. påbud fra Center for Cybersikkerhed.	Vi har fået oplyst, at Nianet ikke har været underlagt evt. påbud fra Center for Cybersikkerhed, hvorfor kontrollen ikke kan testes. Ingen yderligere bemærkninger.