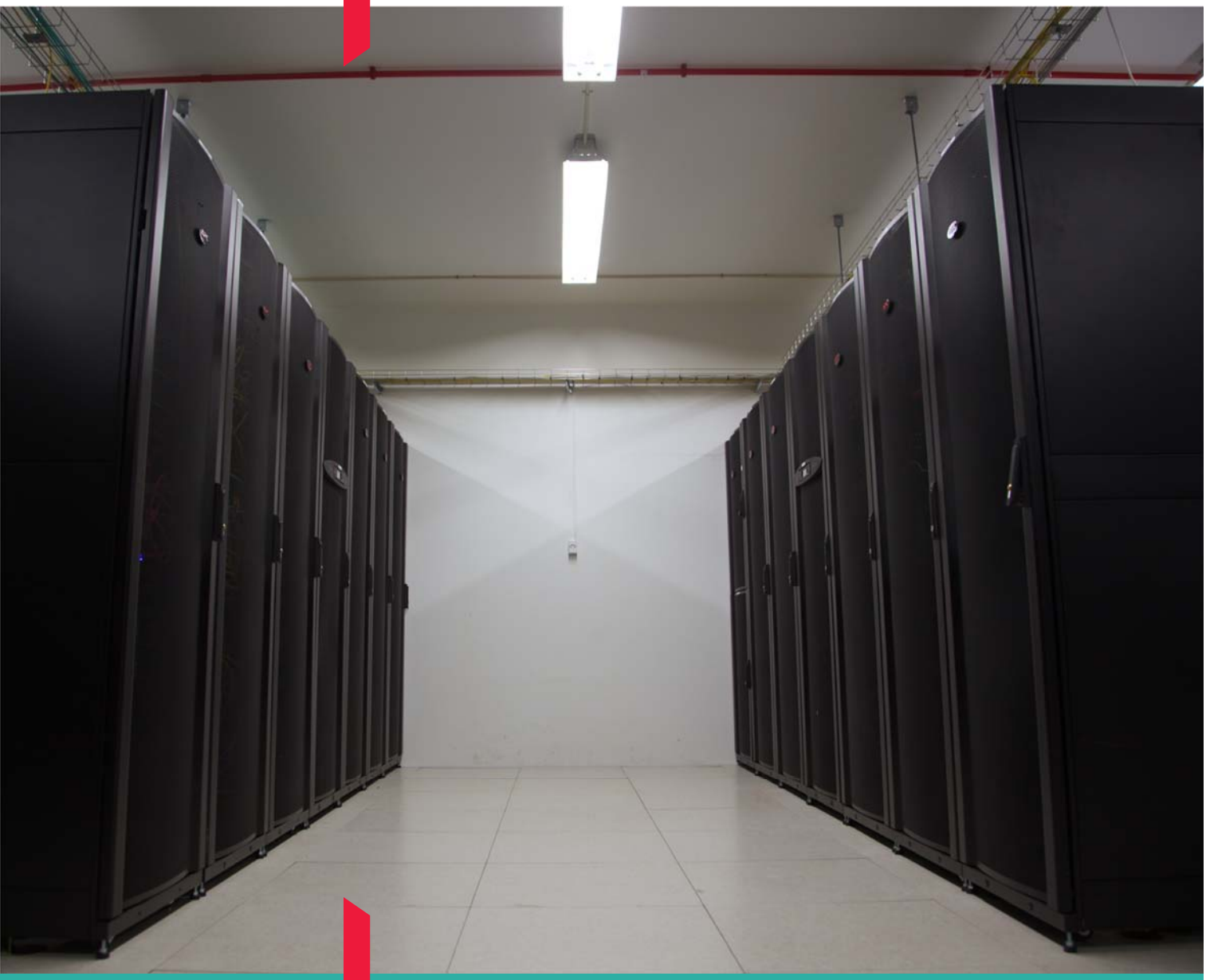


ISAE 3402-ERKLÆRING FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2018 OM BESKRIVELSEN AF KONTROLLER, DERES UDFORMNING OG FUNKTIONALITET I TILKNYTNING TIL DATACENTERLØSNING

GlobalConnect A/S

BDO

INDHOLD

REVISORS ERKLÆRING

UAFHÆNGIG REVISORS ERKLÆRING MED SIKKERHED FOR PERIODEN FRA 1. JANUAR TIL 31. DECEMBER 2018 OM BESKRIVELSEN AF KONTROLLER, DERES UDFORMNING OG FUNKTIONALITET I TILKNYTNING TIL DATACENTERLØSNING

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

Omfang

Vi har fået som opgave at afgive erklæring om GlobalConnect A/S' (serviceleverandøren) beskrivelse på side 5 - 13 af kontroller i tilknytning til Datacenterløsning i hele perioden fra 1. januar til 31. december 2018 (beskrivelsen) og om udformningen og funktionen af de kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Serviceleverandørens ansvar

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

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

Revisors uafhængighed og kvalitetsstyring

Vi har overholdt kravene til uafhængighed og andre etiske krav i International Ethics Standards Board for Accountants' (IESBA) etiske regler, som er baseret på grundlæggende principper om integritet, objektivitet, faglige kompetencer og fornøden omhu, fortrolighed samt professionel adfærd.

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

Revisors ansvar

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

En erklæringsopgave med sikkerhed om at afgive erklæring om beskrivelsen samt 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 beskrivelsen ikke er retvisende, og 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 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 serviceleverandøren har specificeret og beskrevet på side 4.

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

Begrænsninger i kontroller hos en serviceleverandør

Serviceleverandørens beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og omfatter derfor ikke nødvendigvis alle de aspekter i løsningen, som hver enkelt kunde måtte anse for vigtigt efter deres særlige forhold. Endvidere vil kontroller hos en serviceleverandør, som følge af deres art, muligvis ikke forhindre eller opdage alle fejl. 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 serviceleverandørens udtalelse på side 4. Det er vores opfattelse:

a. at beskrivelsen af kontroller i tilknytning til Datacenterløsning, således som disse var udformet og implementeret i hele perioden fra 1. januar til 31. december 2018 i alle væsentlige henseender er retvisende, og

b. at kontrollerne, som knytter sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden fra 1. januar til 31. december 2018, og

c. at de testede kontroller, som var de kontroller, der var nødvendige for at give høj grad af sikkerhed for, at kontrolmålene i beskrivelsen blev nået i alle væsentlige henseender, har fungeret effektivt i hele perioden fra 1. januar til 31. december 2018.

Beskrivelse af test af kontroller

De specifikke kontroller, der er blevet testet, og resultater af disse test, fremgår på side 15 – 33.

Tiltænkte brugere og formål

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

København, den 14. februar 2019

BDO Statsautoriseret revisionsaktieselskab

Per Sloth
Partner, chef for Risk Assurance
Registreret revisor

Lene Yde Poulsen
Director, CISA

GlobalConnect

GLOBALCONNECT A/S' UDTALELSE

GlobalConnect A/S har udarbejdet medfølgende beskrivelse af serviceydelser inden for Datacenterløsninger og de tilhørende kontroller.

Beskrivelsen er udarbejdet til brug for serviceleverandørens kunder 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 væsentlige fejlinformation i kundernes regnskaber.

GlobalConnect A/S bekræfter, at den medfølgende beskrivelse giver en retvisende beskrivelse af serviceydelser inden for Datacenterløsninger og de tilhørende kontroller i hele perioden fra 1. januar til 31. december 2018. Kriterierne for denne udtalelse var, at den medfølgende beskrivelse:

1. Redegør for, hvordan serviceydelserne inden for Datacenterløsninger og tilhørende kontroller var udformet og implementeret, herunder redegør for:
   - De typer af ydelser, der er leveret.
   - De processer i både informationsteknologiske og manuelle systemer, der er anvendt til sikring af fortrolighed, integritet og tilgængelighed af systemer og data.
   - De relevante kontrolmål og de kontrolaktiviteter, der er udformet til at nå disse mål.
   - De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne, kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for kundernes Datacenterløsninger.

2. Indeholder relevante oplysninger om ændringer i serviceydelserne inden for Datacenterløsninger og tilhørende kontroller foretaget i perioden fra 1. januar til 31. december 2018.

3. Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af beskrivelsen af Datacenterløsninger og de tilhørende kontroller under hensyntagen til, at denne beskrivelse er udarbejdet for at opfylde de almindelige behov hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved løsningen og kontrollerne, som den enkelte kunde måtte anse vigtigt efter deres særlige forhold.

GlobalConnect A/S bekræfter, at de kontroller, der knytter sig til de kontrolmål, som er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden fra 1. januar til 31. december 2018. Kriterierne anvendt for at give denne udtalelse var, at:

1. De risici, der truede opnåelsen af de kontrolmål, der er anført i beskrivelsen, var identificeret.

2. De identificerede kontroller ville, hvis udført som beskrevet, give høj grad af sikkerhed for, at de pågældende risici ikke forhindrede opnåelsen af de anførte kontrolmål.

3. Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse, i hele perioden fra 1. januar til 31. december 2018.

Taastrup, den 11. februar 2019

GlobalConnect A/S

Martin Lippert
Administrerende direktør, CEO

GLOBALCONNECT A/S' BESKRIVELSE

OVERORDNET BESKRIVELSE AF GLOBALCONNECT

GlobalConnect udbyder Sort Fiberløsninger, Transmissionsløsninger. Outsourcing Services, herunder cloud services, samt Datacenterløsninger i Danmark, Nordtyskland og dele af Sverige til bl.a. en række nationale og internationale televirksomheder, der servicerer private og offentlige virksomheder, universiteter og uddannelsesinstitutioner. Herudover leveres service til danske virksomheder.

GlobalConnects vision er at blive den førende tele- og datakommunikations serviceleverandør i Danmark og Nordtyskland og en nøglespiller i de markeder, vi opererer i.

Nærværende beskrivelse omfatter serviceydelser inden for Datacenterløsninger. Kontroller vedrørende Sort Fiber- og Transmissionsløsning er afdækket af en særskilt ISAE 3402 type 2-erklæring for perioden fra 1. januar til 31. december 2018 om beskrivelsen af disse kontroller, deres udformning og funktionalitet, og de er derfor ikke en del af denne beskrivelse.

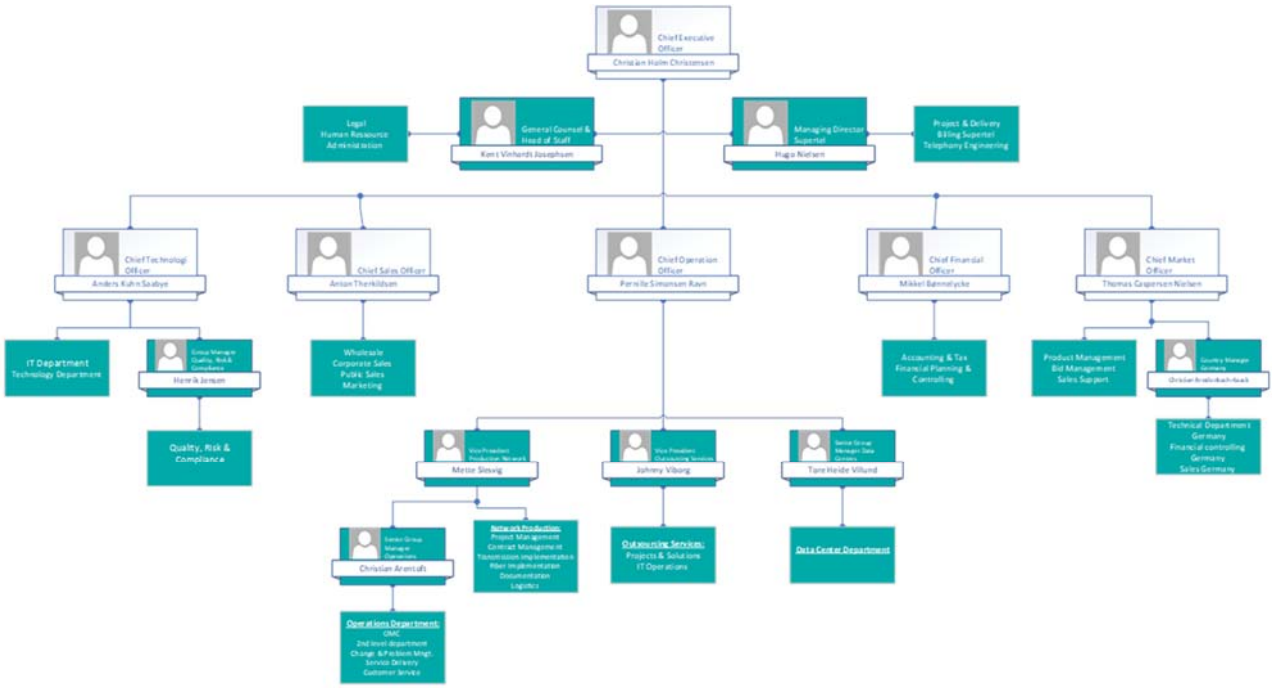
OVERORDNET BESKRIVELSE AF GLOBALCONNECTS ORGANISATION

Internt er GlobalConnect organiseret således med:

- En Ledelse bestående af 5 direktører, der udgør den øverste ledelse i selskabet.
- En Salgsorganisation med kontorer i Taastrup, Stilling, Odense og Hamborg.
- En Product Management- og Salgssupport-afdeling.
- En marketingafdeling
- En produktionsafdeling med underopdeling i Fiberimplementering, Transmissionsimplementering, Logistikafdeling, Project Management og Contract Management.
- En datacenterafdeling med alle Global Connects Datacenter drifts-, vedligeholdelses- og anlægsaktiviteter fordelt i Taastrup, Stilling og Hamborg.
- En outsourcing-afdeling, som varetager design og drift af cloud og outsourcing ydelser.
- En driftsafdeling med OMC, 2nd level operations, Infrastructure Development, Service Delivery afdeling sat en Change Management afdeling.
- En it-afdeling med Operations and Support, Business Support Systems and Operations Support system.
- Stabsfunktioner for Finans, HR, Legal samt Administration.
- En Quality, Risk & Compliance-afdeling.
- Datterselskaber, som udbyder telerelaterede services typisk baseret på services indkøbt hos GlobalConnect.

GlobalConnect

GlobalConnects organisationsdiagram pr. 1. august 2018:



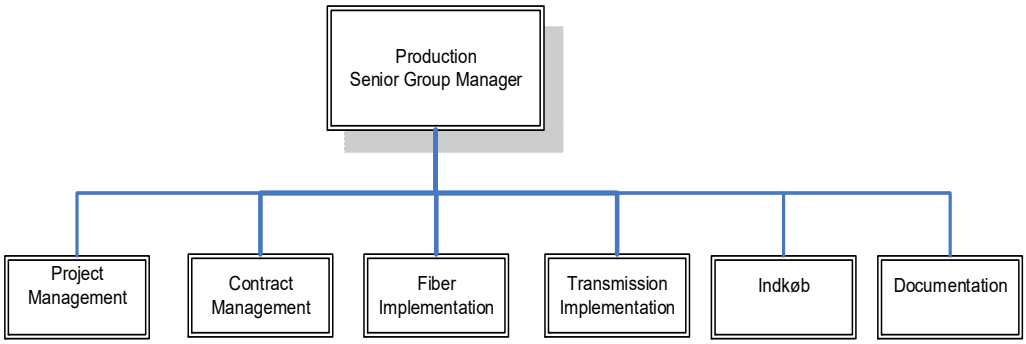
Nedenfor er de aktuelle organisationsbeskrivelser for GlobalConnect.

Produktionsafdelingen

GlobalConnect har organisatorisk inddelt produktionsafdelingen i en implementeringsafdeling for fiber og transmission – internt benævnt Production - og en serviceafdeling opdelt i en enhed for Project Management og en enhed for Contract Management. Logistikfunktionen er ligeledes en del af Produktionsafdelingen.

Implementeringsorganisationen

Implementeringsorganisationen huser projektlederne og har ansvaret for projektet, indtil det idriftsættes. Når projektet er idriftsat, overgår det overordnede ansvar til driftsorganisationen. Der er tilknyttet ca. 50 personer til implementeringsorganisationen.



Project Management - Overordnet ansvar for projektkoordinering samt kommunikation under projekternes gennemførelse. Der udføres koordinering internt og eksternt i forbindelse med alle implementeringsforløb. Project Management vil altid være orienterede og opdaterede på det aktuelle forløb af projekter.

Contract Management - Ansvar for validering af kontrakt med henblik på fakturering og debitorhåndtering.

Fiber Implementation – Gravearbejde: Kortlægning af trace, undersøgelse af eksisterende rør- og ledningsføring og myndighedsbehandling. Herefter udarbejdelse af kravspecifikationer, kontrahering, styring af entreprenører, tilsyn og aflevering. Projektledelse, styring af tid, økonomi, leverandører, ansvar for fremdrift og kvalitet i opgaven. Herunder kommunikation med kunden, myndigheder, leverandører, entreprenører samt evt. slutbrugere.

I forbindelse med gravninger benyttes underleverandører til gravning og underboring. Splidsning af fibre foretages primært af GlobalConnect A/S' personale, men i spidsbelastninger kan der benyttes underleverandør til splidsning af nye fiberstrækninger samt planlagte omlægninger i nettet.

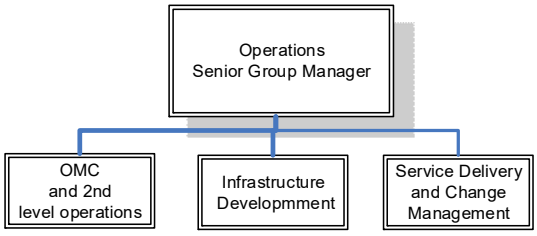
Transmission Implementation - Netværksdelen, herunder kravspecifikation, opsætning af aktivt udstyr, krav til kvalitet og test, udbud og aflevering. Projektledelse, styring af tid, økonomi, leverandører, ansvar for fremdrift og kvalitet i opgaven, herunder kommunikation med kunden, myndigheder, leverandører, entreprenører samt evt. slutbrugere.

Dokumentation – Dokumentation af alle fibre med tilhørende forbindelser i GlobalConnect A/S' benyttede GIS programmer Cross, MapInfo og ConnectMaster.

Logistik – Ansvar for håndtering af indkøb til projektgennemførelse med speciel fokus på GlobalConnect A/S' strategisk vigtige leverandører.

Alle afdelinger består udelukkende af interne ansatte i GlobalConnect A/S. Medarbejderne er kompetente og erfarne på hver deres arbejdsområde, da størstedelen har mange års erfaring med arbejde inden for telekommunikation.

Driftsafdelingen (Operations)



Der er tilknyttet ca. 30 personer til driftsafdelingen, som står for den daglige drift og overvågning af fiber- og transmissionsnet samt datahaller og forstærkersites samt udvikling og vedligeholdelse af GlobalConnect A/S' transmissionsinfrastruktur. Endvidere varetager driftsafdelingen kvalitetsledelse, serviceledelse over for kunder samt håndtering af planlagt arbejde i hele organisationen.

OMC og 2nd level support – Døgnbemandet driftscenter, der overvåger, drifter og vedligeholder alle platforme. Desuden Single Point of Contact for alle idriftsatte leverancer. Teknikere fra "Transmission" udfører fejlretning mv. for Operations & Maintenance (OMC), der har ansvaret for driften.

Infrastructure Development/3rd level support - Ansvar for udbygning og vedligeholdelse af GlobalConnect A/S' backbone netværk samt håndtering af komplekse hændelser.

Service Delivery og Change Management – Rapportering og løbende service level håndtering over for kunder, test og accept af løsninger, der leveres til kunderne samt overordnet planlægning og håndtering af change management (planlagt arbejde i nettet).

Beskrivelse af serviceorganisationen

I dagtimerne er der tre - seks operatører i OMC'en til betjening af kunder på first level support, medarbejdere med ansvar for planlagt arbejde i forbindelse med f.eks. omlægning af fibre samt en teknisk specialist til bl.a. håndtering af nye løsninger til drift. Uden for normal arbejdstid er der minimum én operatør i OMC'en.

På second level support, via vores tekniske organisation, rådes der over seks ansatte. På third level support, via vores infrastrukturenhed, rådes der over seks ansatte.

På third level support rådes der over landsdækkende backup aftaler ved fiberbrud og 2 tilsvarende landsdækkende aftaler ved strømopgaver. GlobalConnect A/S ligger til enhver tid inde med reserveudstyr, der hurtigt kan udskiftes med defekt udstyr.

Ved fiberarbejde benyttes der graveentreprenører til gravning af tracé, rørlægning og ispuling af fibre. For nye fiberstrækninger benyttes der desuden entreprenører til splidsning af fibrene, mens der ved fejlretning på eksisterende fiberanlæg primært benyttes egne ressourcer.

Beskrivelse af Quality, Risk & Compliance

Afdelingen varetager identificering og beskrivelse af kvalitets- og informationssikkerhedsparametre, vedligeholdelse og kontinuerlig optimering af et ISO 9001-baseret kvalitetsledelsessystem, implementering af kvalitets- og informationssikkerhedsparametre i organisationen, herunder gennemførelse og evaluering af intern audit. Afdelingen håndterer endvidere beredskabsøvelser, Risk Management-opgaver, myndighedsforhold omkring informationssikkerhed og social ansvarlighed.

OVERORDNET BESKRIVELSE AF DATACENTERLØSNING I DANMARK OG NORDTYSKLAND

Datacenterløsningerne er en vigtig del af i GlobalConnects udbud af teleservices, fordi datacenter og fibernet spiller sammen, når det gælder om at give kunderne effektive driftsbetingelser for it-tjenester.

Datacenterløsningerne består af serverrum, hvor det er muligt at opsætte egne racks i et egnet driftsmiljø for servere og andet it- og teleudstyr. Kunder har adgang til faciliteterne 24/7/365.

Høj fysisk sikkerhed prioriteres højt. Porte, hegn, indbrudssikring og overvågning er vigtige elementer, når installationerne skal sikres imod uvedkommendes adgang. Alle adgange logges i ADK-systemet.

Datacenterløsningerne er opbygget med N+1 redundans på alle kritiske systemer, for eksempel er strømforsyning sikret af redundante UPS og dieseldrevne generatorer. Køleanlæggene er ligeledes redundante. Hændelser bliver registreret i Service Management Systemet.

Datacentrene er placeret ved knudepunkterne på GlobalConnects netværksrygrad af fiberringe, som danner et stort 8-tal hen over Danmark, Sverige og Nordtyskland. Netværkets indbyggede redundans sikrer høj transmissionssikkerhed og oppetid for kunders it-tjenester og sikrer desuden, at kommunikationsretningen kan vendes i tilfælde af kabelbrud eller nedbrud af transmissionsudstyr.

GlobalConnect har datacentre fordelt i både Danmark og Tyskland

- 20 haller Taastrup
- 6 haller Hamborg
- 4 haller Kolding
- 3 haller Aarhus
- 1 hal Albertslund
- 1 hal indre København
- 1 hal København NV
- 1 hal Odense

Overvågning af datacenterløsningerne fra et døgnbemandet driftscenter

GlobalConnects OMC – Operations & Maintenance Centre – i Taastrup overvåger Datacenterløsningerne nøje, bl.a. også med videoovervågning af indgange og porte til områderne. OMC'en er bemandet 24/7/365.

Høj sikkerhed opnås bl.a. ved personlig adgangskontrol, døgnovervågning fra OMC, inklusive bl.a. videoovervågning, avancerede brand- og indbrudsalarmer. Begivenhed eller alarm, lige fra adgangskontrol til udsving i lufttemperatur, undersøges med det samme. Strømforsyning sikres af redundante UPS og dieseldrevne generatorer, og også køleanlæggene er redundante.

GlobalConnect anvender et Service Management System til registrering og opfølgning samt dokumentation af hændelser i såvel interne it-systemer som kundevendte løsninger. Dette øger i væsentlig grad sikkerheden i håndtering af fejl og nedbrud, som rapporteres af kunderne, eller som konstateres i forbindelse med døgnovervågningen.

BESKRIVELSE AF DET OVERORDNEDE KONTROLMILJØ

GlobalConnects kontrolmiljø afspejler den stilling, som ledelsen har taget til betydning af risici, kontroller og den vægt, der lægges på kontroller i politikker, processer, procedurer, metoder og den organisatoriske struktur.

GlobalConnects Q&ISMS er opbygget, så det lever op til kravene i den internationale standard ISO/IEC ISO 27001. Det tilhørende kontrolmiljø til løbende forbedringer og forebyggende foranstaltninger varetages af QRC under ledelse af en informationssikkerheds- og kvalitetschef. Der holdes løbende møder i GlobalConnects Kvalitets- og IT-sikkerhedsudvalg (KSU), som består af nøglemedarbejdere fra flere forskellige områder i organisationen.

Udvalgets formål er på et taktisk niveau at behandle emner indenfor kvalitet og/eller it-sikkerhed. Emner, der skal eskaleres i forhold til gennemførelse, bringes op i GlobalConnects Kvalitets- og IT-sikkerhedsforum (QSB). Dette forum består af 2 direktører, en vicedirektør samt Senior Group Managers fra henholdsvis Operations samt GlobalConnect-Outsourcing Services og kvalitetscheferne fra disse to enheder. På disse møder udstikker ledelsen desuden retningslinjer og mål for det fortsatte kvalitetsarbejde i GlobalConnect.

Auditplan for gennemgang af forretningsprocesser opdateres hvert år ved årsskiftet og skal godkendes af QSB, og handlingsplan for håndtering af uønskede risici udarbejdes.

RISIKOVURDERING

Der gennemføres en årlig risikovurdering, og input til denne vurdering indhentes fra alle niveauer i organisationen og gennem lov- og myndighedskrav. Processen faciliteteres af et kvalitets- og sikkerhedsudvalg bestående af ledende medarbejder fra relevante afdelinger. Vurderingen forelægges til godkendelse af den øverste ledelse. Der udarbejdes ligeledes årligt en beredskabsplan, som afspejler det gældende trusselsbillede.

Risikovurderinger tager udgangspunkt i implementeringsvejledningerne i den internationale standard ISO27002.

GlobalConnect udfører løbende aktiviteter, der skal:

- Kortlægge og gruppere GlobalConnects samlede infrastruktur (transmissions- og kabelveje bygninger m.v.),
- Identificere, hvilke trusler der udgør de væsentligste risici,
- Identificere, udvælge og prioritere beredskabet over for disse risici.

Sandsynlighed og konsekvens for truslerne revurderes ud fra de informationer, der er til rådighed på indeværende tidspunkt. Disse er tilsammen et udtryk for trusselsniveauet. Hvor trusselsniveauet er lavt, er der mindre behov for sikringsforanstaltninger, end hvor trusselsniveauet er højt. Når trusselsniveauet er fastsat, vurderes det i hvor høj grad sikringsmiljøet tager højde for det pågældende trusselsniveau, og deraf kan det udledes hvor stor den aktuelle restrisiko er.

Den daglige ledelse i GlobalConnect tager ud fra risikovurderingen stilling til, om en identificeret risiko kan accepteres, skal nedbringes eller om der eventuelt skal forsikres ud af udvalgte risici.

Kritiske risici er gennemgået med henblik på at vurdere sårbarheder i relation til de forebyggende foranstaltninger, der allerede er foretaget for at imødegå truslerne. For de risici, som er vurderet som uacceptable, er der udarbejdet en samlet handlingsplan til håndtering af risici.

Der gennemføres løbende forebyggende og forbedrende foranstaltninger til begrænsning af kendte trusler og sårbarheder.

For en beskrivelse af kontrolmål og kontroller for risikovurdering i forhold til Datacenterløsninger henvises der til område A.4 under kontrolmål, kontroller, test og resultat af test, der er en integreret del af denne beskrivelse.

KONTROLMÅL OG KONTROLLER FOR DATACENTERLØSNING

Kontrolmål og kontroller for Datacenterløsning er fastlagt for de nedenfor anførte områder i overensstemmelse med det overordnede kontrolmiljø, baseret på den internationale standard ISO/IEC ISO 27001/27002. Beskrivelsen af kontrolmål og kontroller for disse områder under kontrolmål, kontroller, test og resultat af test er en integreret del af denne beskrivelse.

- A.5: Informationssikkerhedspolitik
- A.6: Organisation af informationssikkerhed
- A.7: Personalesikkerhed
- A.9: Adgangsstyring
- A.11: Fysisk sikring og miljøsikring
- A.12: Driftssikkerhed
- A.16: Styring af informationssikkerhedsbrud
- A.17: Informationssikkerhedsaspekter ved nød–, beredskabs- og retableringsstyring

A.5 Informationssikkerhedspolitikker

GlobalConnect har formuleret en formel informationssikkerhedspolitik. Den udleveres ved ansættelsen, og alle medarbejdere er underlagt krav om, at de ajourfører sig periodisk i forhold til informationssikkerhedspolitik med tilhørende håndbøger. Endelig gøres vores leverandører/samarbejdspartnere ligeledes bekendt med informationssikkerhedspolitikken i forbindelse med rekvirering af fortrolighedserklæringer. Informationssikkerhedspolitikken revurderes årligt af ledelsen.

A.6 Organisation af informationssikkerhed

GlobalConnect har etableret kontroller som sikrer, at der er etableret en overordnet styring af informationssikkerheden herunder en delegering af ansvar samt en håndtering af væsentlige risici i overensstemmelse med krav fra virksomhedens ledelse.

Ledelsens forpligtelse til informationssikkerhed
Ledelsen tager aktivt del i informationssikkerheden i organisationen. Det formelle ansvar, herunder godkendelse af informationssikkerhedspolitikken, ligger således også hos CEO.

Koordinering af informationssikkerheden
Aktiviteter til sikring af informationssikkerheden behandles i et tværorganisatorisk Kvalitets- og Sikkerhedsudvalg (KSU) med deltagelse fra alle relevante afdelinger.

Placering af informationssikkerhedsansvar
Alle ansvarsområder for informationssikkerheden er beskrevet i GlobalConnects sikkerhedspolitik, hvoraf der fremgår en klar ansvarsplacering i forbindelse med informationssikkerhed og beredskabsplanlægningen.

A.7 Personalesikkerhed

GlobalConnect har etableret kontroller, som understøtter, at der er foretaget passende baggrundstjek af ansatte, samt at disse er bevidste om deres opgaver og ansvar i relation til informationssikkerhed.

Nogle kunder har krav om sikkerhedsgodkendelse af vores medarbejdere. En forudsætning for adgangen til kunders it-miljøer er som minimum, at der afleveres en ren straffeattest, og hvor kunder kræver det, en PET godkendelse og/eller en FE godkendelse. PET- og FE godkendelser fornyes af den udstedende myndighed i foruddefinerede intervaller.

Ledelsens ansvar
For medarbejdere gælder det, at de ved ansættelse forpligter sig til at efterleve virksomhedens politikker, herunder sikkerhedspolitikken.

Bevidsthed om informationssikkerhed, uddannelse og træning
For medarbejdere gælder det, at de informeres ved enhver væsentlig ændring i gældende politikker og relevante procedurer. Dette gøres dels på de månedlige møder i kvalitets- og sikkerhedsudvalget, dels på personalemøder.

Fortrolighedserklæringer
Tavshedspligt er en del af ansættelsesaftalerne. For enkelte kunder er der derudover særlige fortrolighеds- og tavshedserklæringer og øvrige sikkerhedsbestemmelser for de medarbejdere, der arbejder med kundernes it-miljøer. Der er desuden udformet en oversigt over alle de love, krav og sikkerhedscirkulærer, som GlobalConnect skal overholde. Oversigten vedligeholdes gennem periodiske reviews.
Forpligtelser i forbindelse med fratrædelser
Generelle vilkår for ansættelse, herunder forhold omkring ophør, er beskrevet i medarbejderens ansættelseskontrakt med tilhørende tro- og love-erklæring. Herudover er der en formel procedure ved fratrædelse, som skal følges af den nærmeste leder. Den HR-ansvarlige har det endelige ansvar herfor.

Tilbagelevering af udstyr
Alle medarbejdere bedes om at aflevere al udleveret materiale, når ansættelseskontrakten ophører. Dette foregår gennem et workflow, forankret hos HR-afdelingen.

Nedlæggelse af adgangsrettigheder
GlobalConnects formelle HR procedurer sikrer, at alle rettigheder og fysiske adgange inddrages, når en ansættelse ophører. Dette sker gennem et workflow, forankret i HR afdelingen. Som en del af vores kvalitetsledelsessystem gennemgås adgange periodisk.

A.9 Adgangsstyring

GlobalConnect har etableret kontroller som sikrer at adgange til systemer og data tildeles via en dokumenteret proces efter relevant arbejdsmæssigt betinget behov herfor og nedlægges, når den pågældende adgang ikke længere er nødvendig.

Brugeroprettelse
GlobalConnect har procedurer for oprettelse og nedlæggelse af brugere, som er forankret i HR afdelingen.

Udvidede rettigheder
Alle rettigheder er styret ud fra medarbejdernes roller og kontrolleres løbende under vores kvalitetsledelsessystem.

Styring af password
Tildeling af passwords er underlagt en række regler, som er opsat i vores Active Directory.

A.11 Fysisk sikring og miljøsikring

GlobalConnects OMC i Taastrup overvåger alle datacentre med blandt andet videoovervågning af indgange og porte til områderne. OMC'en er bemandet 24/7/365.

Høj sikkerhed opnås blandt anet ved personlig adgangskontrol, døgnbemandet 24/7/365 overvågning fra OMC, videoovervågning samt avancerede brand- og indbrudsalarmer. Enhver begivenhed eller alarm undersøges med det samme. Strømforsyning sikres af redundante UPS'er og dieseldrevne generatorer. Køleanlæggene er også redundante. Alle hændelser bliver registreret i Service Management System.

Høj fysisk sikkerhed prioriteres højt. Porte, hegn, indbrudssikring og overvågning er vigtige elementer, når installationerne skal sikres imod uvedkommendes adgang. Alle adgange logges i ADK-systemet.

Alle datacentre, herunder køleanlæg, generatorer, 48-Volts-anlæg, UPS, brandanlæg etc., er underlagt periodiske serviceeftersyn både af GlobalConnects egne teknikere og af eksterne serviceleverandører.

A.12 Driftssikkerhed

GlobalConnect anvender et Service Management System til registrering og opfølgning samt dokumentation af alle ændringer i såvel interne it-systemer som de kundevendte løsninger inden for datacenterløsninger. Dette øger i væsentlig grad sikkerheden i håndtering af fejl og nedbrud, som rapporteres af kunderne, eller som konstateres i forbindelse med døgnovervågningen.

OMC åbner en fejlrapport i Service Management System på alle fejl med et referencenummer, som skal benyttes gennem hele den efterfølgende fejlhåndteringsproces.

Al planlagt arbejde for alle løsninger registreres i Service Management System under egen kategori, og OMC har ansvaret for at udsende varsler til kunder. Disse registreres ligeledes i Service Management System. Henvendelser fra kunder til OMC i den anledning behandles og besvares direkte, og dokumentationen for korrespondancen med kunderne registreres i Service Management System. Efter færdiggørelse og check af driftstilstand færdigmeldes arbejdet i Service Management System.

GlobalConnect anvender Frontsafe A/S som leverandør til al sikkerhedskopiering af driftssystemerne. GlobalConnect efterser, at Frontsafe A/S har dokumenteret sine kontroller i en ISAE 3402 revisorerklæring, som herefter vurderes i forhold til at leve op til GlobalConnects krav til sikkerhedskopiering.

A.16 Styring af informationssikkerhedsbrud

GlobalConnect har etableret kontroller som sikrer, at sikkerhedshændelser håndteres rettidigt samt at der følges op på disse.

Der er etableret processer og procedurer for håndtering af sikkerhedshændelser for at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder som dokumenteres i Service Management System. Styring af sikkerhedshændelser og brud foretages efter fastlagte procedurer defineret i GlobalConnects Q&ISMS' afsnit om hændelses- og krisestyring.

Alle sikkerhedsbrud (security incidents) håndteres i Service Management System og i henhold til etablerede procedurer.

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

GlobalConnect har og vedligeholder beredskabsplaner. Planerne fastlægger ansvaret for opretholdelse af en optimal driftssikkerhed, herunder reaktionstider for forskellige niveauer af kritiske fejl, processen for eskalation, processen for håndtering af krisesituationer samt kommunikation med kunder og medierne i sådanne tilfælde.

Planerne beskriver overordnet specifikationerne for det installerede udstyr til elforsyning, nødgeneratorer, UPS, køling, brandslukning, alarmsystem og adgangskontrol samt de aktiviteter, der udføres for at vedligeholde disse systemer med henblik på løbende forebyggelse og forbedringer.

Der er udarbejdet beredskabsplaner for Datacentre, som opdateres mindst hvert andet år. Der foreligger desuden godkendt plan for afprøvning af disse planer, som er gældende 5 år frem i tiden, og som sikrer forretningens videreførelse ved sikkerhedshændelser. Afprøvningerne dokumenteres i Service Management System.

FORETAGNE ÆNDRINGER I SERVICEYDELSER OG TILHØRENDE KONTROLLER

I perioden fra 1. januar til 31. december 2018 er der ikke foretaget væsentlige ændringer i Global-Connects serviceydelser og tilhørende kontroller inden for Datacenterløsning.

KONTROLMÅL, KONTROLLER, TEST OG RESULTAT AF TEST

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

I testskemaet har vi beskrevet de udførte test, som blev vurderet som nødvendige for at kunne opnå høj grad af sikkerhed for, at de anførte kontrolmål blev opnået, og de tilhørende kontroller fungerede effektivt i perioden fra 1. januar til 31. december 2018.

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

Type	Beskrivelse
Forespørgsel	Forespørgsler hos passende personale hos GlobalConnect er udført for alle væsentlige kontrolaktiviteter. Forespørgslerne blev udført for blandt andet at opnå viden og yderligere oplysninger om indførte politikker og procedurer, herunder hvordan kontrolaktiviteterne udføres, samt at få bekræftet beviser for politikker, procedurer og kontroller.
Inspektion	Dokumenter og rapporter, der indeholder angivelse om udførelse af kontrollen, er gennemlæste med det formål at vurdere udformningen og overvågningen af de specifikke kontroller, herunder om kontrollerne er udformede, således at de kan forventes at blive effektive, hvis de implementeres, og om kontrollerne overvåges og kontrolleres tilstrækkeligt og med passende intervaller. Test af væsentlige systemopsætninger af tekniske platforme, databaser og netværksudstyr er udført for at påse, om kontroller er implementerede, herunder eksempelvis vurdering af logning, sikkerhedskopiering, patch management, autorisationer og adgangskontroller, datatransmission samt besigtigelse af udstyr og lokaliteter.
Observation	Anvendelsen og eksistensen af specifikke kontroller er observeret, herunder test for at påse, at kontrollen er implementeret.
Genudførelse	Kontroller er genudført for at opnå yderligere bevis for, at kontrollen fungerer som forudsat.

For de ydelser, som Frontsafe A/S leverer inden for sikkerhedskopiering af driftssystemerne, har vi fra uafhængig revisor modtaget en ISAE 3402-erklæring for perioden fra 1. oktober 2017 til 30. september 2018 vedrørende tekniske og organisatoriske sikringsforanstaltninger i tilknytning til driften af Cloud Backup-ydelser. Denne serviceunderleverandørs relevante kontrolmål og tilknyttede kontroller indgår ikke i GlobalConnect A/S' beskrivelse af serviceydelser og tilhørende kontroller i tilknytning til drift af Datacenterløsning. Vi har således alene vurderet erklæringen og testet de kontroller hos GlobalConnect A/S, der overvåger funktionaliteten af serviceunderleverandørens kontroller.

A.4: Risikovurdering

Kontrolmål

- *At sikre, at der udføres en årlig risikovurdering som danner grundlag for forretningsmæssigt begrundede implementeringer af kontroller.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Risikovurdering • Der foretages en årlig risikovurdering, som godkendes af ledelsen. Risikovurderingen indgår som en del af arbejdet med GlobalConnects informationssikkerhedsledelsessystem (ISMS).	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens informationssikkerhedspolitik, informationssikkerhedsregler og informationssikkerhedshåndbog. Vi har observeret, at den overordnede risikovurdering indgår som en del af arbejdet med informationssikkerhedsledelsessystemet. Vi har foretaget inspektion af serviceleverandørens risikovurdering. Vi har observeret, at møder i serviceleverandørens kvalitets- og sikkerhedsudvalg løbende er afholdt, og vi har foretaget inspektion af udvalgte mødereferater. Vi har observeret, at møderne har til formål at sikre vedligeholdelse, højnelse og forankring af informationssikkerhed, herunder en løbende vurdering af trusler og risici.	Ingen afvigelser konstateret.

A.5: Informationssikkerhedspolitikker Retningslinjer for styring af informationssikkerhed		
Kontrolmål • *At give retningslinjer for og understøtte informationssikkerheden i overensstemmelse med forretningsmæssige krav og relevante love og forskrifter.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Politikker for informationssikkerhed • Ledelsen fastlægger og godkender politikker for informationssikkerhed, som efter godkendelse offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens informationssikkerhedspolitik, informationssikkerhedsregler og informationssikkerhedshåndbog. Vi har observeret, at informationssikkerhedspolitikken er opbygget efter ISO 27001/27002. Vi har foretaget inspektion af serviceleverandørens kommissorium for det nedsatte kvalitets- og sikkerhedsudvalg, herunder procedurer, der sikrer ledelsesgodkendelse og kommunikation i organisationen. Vi har foretaget inspektion af informationssikkerhedspolitikken og observeret, at denne er underskrevet af ledelsen. Vi har observeret, at informationssikkerhedspolitikken er kommunikeret til medarbejdere og relevante eksterne samarbejdspartnere, og vi har foretaget inspektion af dokumentation herfor.	Ingen afvigelser konstateret.
Gennemgang af politikker for informationssikkerhed • GlobalConnect har udarbejdet og implementeret en procedure, der sikrer en periodisk gennemgang af informationssikkerhedspolitikken. • Der er formuleret en skriftlig informationssikkerhedspolitik, som revurderes årligt. • Informationssikkerhedspolitikken er godkendt af ledelsen.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens auditplan for gennemgang af informationssikkerhedspolitikker, informationssikkerhedsregler og informationssikkerhedshåndbog. Vi har observeret, at den fastlagte auditplan følges, herunder at informationssikkerhedspolitikken er gennemgået og revurderet. Vi har foretaget inspektion af dokumentation herfor. Vi har observeret, at informationssikkerhedspolitikken er godkendt og underskrevet af ledelsen. Vi har foretaget inspektion af dokumentation herfor.	Ingen afvigelser konstateret.

A.6: Organisation af informationssikkerhed
Intern organisering

Kontrolmål

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

Kontrolaktivitet	Test udført af BDO	Resultat af test
Roller og ansvarsområder for informationssikkerhed • Ansvaret for informationssikkerheden i Global-Connect er forankret i ledelsen. • Ledelsen har nedsat et tværorganisatorisk Kvalitets- og Sikkerhedsudvalg, der behandler aktiviteter til sikring af informationssikkerheden. • Ledelsen har udpeget en Kvalitets- og Sikkerheds-chef som overordnet ansvarlig for håndtering af in-formationssikkerhed.	Vi har udført forespørgsel hos passende personale hos service-leverandøren. Vi har foretaget inspektion af serviceleverandørens informati-onssikkerhedspolitik, informationssikkerhedsregler og informati-onssikkerhedshåndbog samt oversigt over den interne organise-ring af informationssikkerhed. Vi har foretaget inspektion af serviceleverandørens kommisso-rium for kvalitets- og sikkerhedsudvalget, procedure for kvali-tets- og sikkerhedsarbejdet samt kvalitetshåndbog, herunder dokumentstyring. Vi har observeret, at møder i serviceleverandørens kvalitets- og sikkerhedsudvalg løbende er afholdt, og vi har foretaget inspek-tion af udvalgte mødereferater. Vi har observeret, at møderne har til formål at sikre vedligeholdelse, højnelse og forankring af informationssikkerhed.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed
Før ansættelsen, under ansættelsen og ansættelsesforholdets ophør eller ændring

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Før ansættelsen • Der foretages et baggrundstjek af alle jobkandidaters baggrund i overensstemmelse med forretningsmæssige krav og den funktion, som medarbejderen skal bestride. • Når kunden eller arbejdsopgaven kræver sikkerhedsgodkendelser, indhentes sådanne for relevante medarbejdere i henhold til fastlagt procedure herfor.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for ansættelse og fratrædelse af medarbejdere. Vi har observeret, at der foretages baggrundstjek som en del af ansættelsesprocessen, og vi har foretaget inspektion af godkendt skabelon for ansættelseskontrakt. Vi har foretaget inspektion af blanket for nye medarbejdere, der blandt andet indeholder oplysninger om, hvilke områder den enkelte skal have adgang til, og hvilke programmer og rettigheder den ansatte skal tildeles. Vi har observeret, at blanketten udstedes af HR og godkendes af nærmeste leder. Vi har foretaget inspektion af oversigt over tiltrådte medarbejdere i 2018, og vi har stikprøvevis udvalgt og foretaget inspektion af dokumentation for nyansatte medarbejdere, der følger serviceleverandørens procedurer herfor, herunder oprettelse af medarbejdere i systemer. Vi har foretaget inspektion af liste over de medarbejdere, der er sikkerhedsgodkendte hos Forsvarets Efterretningstjeneste og hos Politiets Efterretningstjeneste, herunder observeret processen for indhentelse og vedligeholdelse af disse sikkerhedsgodkendelser.	Ingen afvigelser konstateret.
Under ansættelsen • Medarbejdere i GlobalConnect informeres løbende om informationssikkerhedsmæssige forhold og evt. trusler i forhold til deres opgaver. • Medarbejdere i GlobalConnect tilkendegiver ved ansættelsen, at de har læst og accepteret Informationssikkerhedspolitikken og -håndbogen.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens intranet. Vi har observeret, at medarbejderne hos serviceleverandøren holdes opdateret med informationssikkerhedsmæssige forhold og eventuelle trusler i forhold til deres arbejdsområder.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed Før ansættelsen, under ansættelsen og ansættelsesforholdets ophør eller ændring		
Kontrolmål • *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.* • *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.* • *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har foretaget inspektion af publikationer til medarbejderne om udvalgte emner inden for informationssikkerhed og databeskyttelseslovgivningen. Vi har observeret, at publikationerne har indgået i oplysningskampagner mv.	
Fortrolighеds- og hemmeligholdelsesaftaler • Alle medarbejdere, der arbejder med fortrolige data - herunder persondata - har underskrevet en fortrolighedserklæring.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens proces for ansættelse af nye medarbejdere samt godkendt skabelon for ansættelseskontrakt. Vi har observeret, at ansættelseskontrakten indeholder vilkår om tavshedspligt, gældende både under ansættelsesforholdet og ved dets ophør og for såvel interne som kunderelaterede data. Vi har foretaget inspektion af stikprøvevis udvalgte ansættelseskontrakter og observeret, at vilkår om tavshedspligt fremgår, og at ansættelseskontrakten er underskrevet af medarbejderen.	Ingen afvigelser konstateret.
Ansættelsesforholdets ophør eller ændring • Efter ansættelsesforholdets ophør eller ændring inddrages eller ændres adgange og rettigheder i forhold til det funktionsmæssige behov herfor. • Efter ansættelsesforholdets ophør afleveres udleveret udstyr fra den fratrædende medarbejder. • Efter ansættelsens ophør sikrer HR, at procedure for fratrædelse bliver overholdt.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for ansættelse og fratrædelse af medarbejdere. Vi har foretaget inspektion af den anvendte fratrædelsesblanket. Vi har observeret, at OMC/IT og medarbejderen underskriver fratrædelsesblanket for henholdsvis lukning af adgangskort og tilbagelevering af serviceleverandørens fysiske udstyr. Fratrædelsesblanketten opbevares i fysisk arkiv hos HR-chefen.	Ingen afvigelser konstateret.

A.7: Personalesikkerhed
Før ansættelsen, under ansættelsen og ansættelsesforholdets ophør eller ændring

Kontrolmål

- *At sikre, at medarbejdere og kontrahenter forstår deres ansvarsområder og er egnede til de roller, de er tiltænkt.*
- *At sikre, at medarbejdere og kontrahenter er bevidste om og lever op til deres informationssikkerhedsansvar.*
- *At beskytte organisationens interesser som led i ansættelsesforholdets ændring eller ophør.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af oversigt over fratrådte medarbejdere i 2018, og vi har foretaget inspektion af fratrædelsesblanket for stikprøvevis udvalgt fratrådte medarbejdere, der følger serviceleverandørens procedurer herfor, herunder nedlæggelse af medarbejdere i systemer.	

A.9: Adgangsstyring Forretningsmæssige krav til adgangsstyring, administration af brugeradgang, brugernes ansvar og styring af system- og applikationsadgang		
Kontrolmål • *At begrænse adgangen til information og informationsbehandlingsfaciliteter.* • *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.* • *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.* • *At forhindre uautoriseret adgang til systemer og applikationer.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Politik for adgangsstyring • Der er vedtaget processer og procedurer for at styre adgange og begrænsninger til systemer og data på grundlag af forretnings- og funktionsmæssige behov. • Alle adgange og ændringer af adgange til systemer og data følger de vedtagne processer og procedurer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for ansættelse og fratrædelse af medarbejdere, procedure for adgangskontrol til fysiske lokationer og systemer samt procedure for ledsaget adgang til serviceleverandørens datacentre. Vi har på baggrund af inspektion af dokumentation for de efterfølgende områder under A.9 observeret, at de vedtagne processer og procedurer efterleves.	Ingen afvigelser konstateret.
Brugerregistrering og -afmelding • GlobalConnect har etableret og følger processen for oprettelse og afmelding af brugere i systemer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for ansættelse og fratrædelse af medarbejdere. Vi har foretaget inspektion af blanket for nye medarbejdere og fratrædelsesblanket. Vi har foretaget inspektion af oversigt over til- og fratrådte medarbejdere i 2018, og vi har stikprøvevis udvalgt og foretaget inspektion af dokumentation for nyansatte og fratrådte medarbejdere, der følger serviceleverandørens procedurer herfor, herunder oprettelse og nedlæggelse af medarbejdere i systemer.	Ingen afvigelser konstateret.
Tildeling, justering og inddragelse af adgangsrettigheder • GlobalConnect har etableret en procedure for tildeling af brugeradgang med henblik på at tildele adgangsrettigheder for alle brugertyper til alle systemer og tjenester.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for ansættelse og fratrædelse af medarbejdere.	Ingen afvigelser konstateret.

A.9: Adgangsstyring
Forretningsmæssige krav til adgangsstyring, administration af brugeradgang, brugernes ansvar og styring af system- og applikationsadgang

Kontrolmål

- *At begrænse adgangen til information og informationsbehandlingsfaciliteter.*
- *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.*
- *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.*
- *At forhindre uautoriseret adgang til systemer og applikationer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
• GlobalConnect har etableret en proces for inddragelse eller justering af adgangsrettigheder, herunder sletning af medarbejders adgang ved flytning eller fratrædelse.	Vi har foretaget inspektion af blanket for medarbejdere, der blandt andet indeholder oplysninger om, hvilke områder den enkelte skal have adgang til, og hvilke programmer og rettigheder den ansatte skal tildeles. Vi har observeret, at blanketten udstedes af HR og godkendes af nærmeste leder. Vi har foretaget inspektion af adgangskontrollister (whitelists) for en stikprøve af serviceleverandørens kunder. Vi har foretaget inspektion af den anvendte fratrædelsesblanket. Vi har foretaget inspektion af oversigt over til- og fratrådte medarbejdere i 2018, og vi har stikprøvevis udvalgt og foretaget inspektion af dokumentation for nyansatte og fratrådte medarbejdere, der følger serviceleverandørens procedurer herfor, herunder tildeling af adgang til systemer og tjenester.	
Styring af privilegerede adgangsrettigheder • GlobalConnect har etableret tildeling af administrativ adgang til enheder i forhold til det funktionsmæssige behov, som er autoriseret. • GlobalConnect har etableret logning af adgange med privilegerede konti (administrative rettigheder).	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedure for ansættelse og fratrædelse af medarbejdere. Vi har foretaget inspektion af blanket for medarbejdere, der blandt andet indeholder oplysninger om, hvilke områder den enkelte skal have adgang til, og hvilke programmer og rettigheder den ansatte skal tildeles, herunder tildeling af administrative adgange. Vi har observeret, at blanketten udstedes af HR og godkendes af nærmeste leder. Vi har foretaget inspektion af oversigt over tiltrådte medarbejdere i 2018, og vi har stikprøvevis udvalgt og foretaget inspektion af dokumentation for nyansatte medarbejdere, der følger serviceleverandørens procedurer herfor, herunder tildeling af adgang til systemer og tjenester.	Ingen afvigelser konstateret.

A.9: Adgangsstyring Forretningsmæssige krav til adgangsstyring, administration af brugeradgang, brugernes ansvar og styring af system- og applikationsadgang		
Kontrolmål • *At begrænse adgangen til information og informationsbehandlingsfaciliteter.* • *At sikre adgang for autoriserede brugere og forhindre uautoriseret adgang til systemer og tjenester.* • *At gøre brugere ansvarlige for at sikre deres autentifikationsinformation.* • *At forhindre uautoriseret adgang til systemer og applikationer.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har foretaget inspektion af auditpolitikken i serviceleverandørens netværksoperativsystem, der sikrer logning af adgang fra brugere med privilegerede/administrative rettigheder.	
Styring af adgangskoder til brugere • GlobalConnect har etableret proces og regler for tildeling og styring af adgangskoder. • GlobalConnect har etableret regler til etablering af adgangskoder, som skal følges af alle medarbejdere.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens informationssikkerhedsregler og informationssikkerhedshåndbog vedrørende brugen af adgangskoder, herunder procedure for brugeradgang til it-systemer. Vi har foretaget inspektion af adgangskodepolitikken og auditpolitikken i serviceleverandørens netværksoperativsystem. Vi har observeret, at der er opsat styring af adgangskoder. Vi har inspiceret udtræk af brugeropsætninger fra serviceleverandørens Active Directory og genudført kontrollen for adgangskodeord. Vi har observeret, at reglerne for adgangskoder følges af alle medarbejdere.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring
Sikre områder og udstyr

Kontrolmål

- *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.*
- *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Fysisk perimetersikring • Den etablerede fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedurer for adgangskontrol og ledsaget adgang til lokaliteter. Vi har foretaget inspektion af den fysiske perimetersikring vedrørende kontorbygninger samt udvalgte datacentre. Vi har ved stikprøver observeret håndteringen af gæstekort og foretaget inspektion af dokumentationen for de udvalgte stikprøver.	Ingen afvigelser konstateret.
Fysisk adgangskontrol • Der er etableret adgangskontroller, som forebygger sandsynligheden for uautoriseret fysisk adgang til, beskadigelse og forstyrrelse af GlobalConnects lokaler og informationer, herunder sikring af, at kun autoriserede personer har adgang. • Aktiviteter registreres i adgangskontrolsystemet i OMC. • Halvårlig gennemgang af eksterne adgangskort, der ikke har været i brug indenfor de seneste 6 måneder, er udført. • Halvårlig gennemgang af interne adgangskort, der ikke har været i brug indenfor de seneste 6 måneder, er udført. • Stikprøvekontrol af udvalgte adgangspunkter i forhold til, om rette personer har rette adgange.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedurer for adgangskontrol og ledsaget adgang til lokaliteter samt procedure for adgangsstyring ved ansættelser og fratrædelser af medarbejdere. Vi har observeret, at medarbejderes fysiske adgangsrettigheder tildeles ud fra arbejdsbetingede behov, og at styringen af disse adgangsrettigheder sker i OMC. Vi har foretaget inspektion af dokumentation herfor. Vi har observeret, at der udføres en månedlig kontrol af, at alle fratrådte medarbejderes adgange er blevet nedlagt. Vi har udtaget en stikprøve og foretaget inspektion heraf. Vi har foretaget inspektion af stikprøvevis udvalgte oprettelse og nedlæggelse af adgange for medarbejdere. Vi har foretaget inspektion af udtræk fra adgangskontrolsystemet og inspektion af nøgleliste over fysiske nøgler. Vi har observeret de etablerede adgangskontroller.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring Sikre områder og udstyr		
Kontrolmål • *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.* • *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har observeret procedure for ledsaget adgang og ved stikprøve foretaget inspektion af dokumentation herfor i Service Management System. Vi har observeret procedure for kunders og leverandørers adgang, herunder adgang som gæst eller adgang til administrative områder. Vi har foretaget inspektion af udvalgte oprettelser og nedtagninger af kunder og leverandørers adgange. Vi har foretaget inspektion af udtræk fra adgangskontrolsystemet. Vi har observeret de etablerede adgangskontroller. Vi har foretaget inspektion af serviceleverandørens halvårlige gennemgang af eksterne og interne adgangskort, der ikke har været i brug inden for de seneste 6 måneder.	

Beskyttelse mod eksterne og miljømæssige trusler
• GlobalConnect overholder specificerede krav til fysisk sikkerhed for datacenterløsninger omfattende følgende forhold:
  • Bygning
  • Gulve
  • Foot-prints
  • Klima
  • Strøm
  • Adgang
  • Alarmmonitering
  • Brandslukning
  • Kabling
	Vi har udført forespørgsel hos passende personale hos serviceleverandøren.
	
	Vi har foretaget inspektion af serviceleverandørens informationssikkerhedspolitik, informationssikkerhedsregler og informationssikkerhedshåndbog.
	
	Vi har foretaget inspektioner og observationer af de fysiske sikkerhedsforanstaltninger for udvalgte datacentre. Vi har observeret, at de indførte fysiske sikkerhedsforanstaltninger er baseret på konkrete risikovurderinger for det enkelte datacenter.
	
	Vi har observeret, at datacentrene er beliggende i indhegnede industriområder, hvortil der kræves nøglekort og kode til døre og porte. Vi har observeret, at adgangen og indgangspartiet til datacentrene og selve datacentrene er kameraovervåget.
		Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring Sikre områder og udstyr		
Kontrolmål • *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.* • *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har observeret, at døre til datacentrene er brandsikrede, og at lofterne er beklædt med brandhæmmende materiale. Vi har observeret, at der er etableret automatisk brandslukningsudstyr i datacentrene, at gulvene er hævet og belagt med antistatisk gulvbelægning, og at fugtfølere er installeret under de hævede gulve. Vi har observeret, at der er installeret redundante køleanlæg i datacentrene, som årligt services og vedligeholdes. Vi har observeret, at der er installeret alarmer for vand, fugt, røg og temperatur, og at alle alarmerne går til OMC. Vi har observeret, at der er én strømindføring tilknyttet til hvert datacenter, og at strømmen og fiber er trukket under det hævede gulv eller placeret i kabelbakker under loftet.	
Arbejde i sikre områder • GlobalConnect har etableret overvågning i datacentre og passende sikring af retningslinjer for færden og arbejde på områderne.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens informationssikkerhedspolitik, informationssikkerhedsregler og informationssikkerhedshåndbog. Vi har foretaget inspektion af udvalgte fysiske datacentre og observeret, at der på de datacentre, som er lokaliseret i fysiske bygninger, er installeret overvågningskameraer, og at datacentrene overvåges af OMC. Vi har observeret, at der sker overvågning hele døgnet af gangarealer i datacentre. Vi har foretaget inspektion af serviceleverandørens fysiske adgangskontrol og beskyttelsesforanstaltninger mod eksterne og miljømæssige trusler.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring Sikre områder og udstyr		
Kontrolmål • *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.* • *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Placering og beskyttelse af udstyr • GlobalConnect har etableret passende foranstaltninger for at forhindre uautoriseret adgang til kunders systemer, data og informationer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedurer for adgangskontrol og ledsaget adgang til lokaliteter samt procedure for adgangsstyring ved ansættelser og fratrædelser af medarbejdere. Vi har foretaget inspektion af udvalgte fysiske datacentre og observeret, at indgang til et datacenter kræver adgangskort med personlig kode, og at indgangen og gangarealer er forsynet med overvågningskamera med bemandet døgnovervågning. Vi har foretaget inspektion af serviceleverandørens fysiske adgangskontrol og beskyttelsesforanstaltninger mod eksterne og miljømæssige trusler.	Ingen afvigelser konstateret.
Understøttende forsyninger (forsyningssikkerhed) • GlobalConnect har etableret og vedligeholder udstyr, som sikrer, at konsekvenser for driftsafbrydelse afbødes. • Der tjekkes for etableret ventilation, kabelbakker m.m. i henhold til fast skabelon for eftersyn (vedligeholdelsesrapport) af datacentre. • GlobalConnect gennemgår vedligeholdelsesrapporter.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af procedure for planlagt arbejde for de enkelte datacentre i Service Management System. Vi har foretaget inspektion af dokumentation for stikprøvevis udvalgte månedlige vedligeholdelsesrapporter fra datacentre. Vi har foretaget inspektion af liste over eksterne leverandører og stikprøvevis inspiceret service- og vedligeholdelsesrapporter fra disse leverandører vedrørende de indførte sikkerhedsforanstaltninger i datacentre.	Ingen afvigelser konstateret.

A.11: Fysisk sikring og miljøsikring Sikre områder og udstyr		
Kontrolmål • *At forhindre uautoriseret fysisk adgang til samt beskadigelse og forstyrrelse af organisationens information og informationsbehandlingsfaciliteter.* • *At undgå tab, skade, tyveri eller kompromittering af aktiver og driftsafbrydelse i organisationen.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Vedligeholdelse af udstyr • GlobalConnect foretager månedsvis forebyggende tilsyn af datacenterfaciliteter. Resultatet af disse tilsyn dokumenteres i udfyldte skemaer. • GlobalConnect har etableret periodisk vedligeholdelse af brandslukningsanlæg, køleanlæg og generatorer i datacentre af eksterne serviceleverandører.	Vi har udført forespørgsler hos passende personale og inspiceret procedurebeskrivelser, interne kontroller og standardaftaler. Vi har foretaget inspektion af procedure for planlagt arbejde for de enkelte datacentre i Service Management System. Vi har foretaget inspektion af dokumentation for stikprøvevis udvalgte månedlige vedligeholdelsesrapporter fra datacentre. Vi har foretaget inspektion af liste over eksterne leverandører. Vi har observeret, at serviceleverandøren har indgået årlige serviceaftaler vedrørende eftersyn af køleanlæg, dieselgenerator, UPS-anlæg og det automatiske brandslukningsudstyr. Vi har foretaget inspektion af serviceaftalerne. Vi har stikprøvevis inspiceret service- og vedligeholdelsesrapporter fra leverandører vedrørende de indførte sikkerhedsforanstaltninger i datacentre.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed
Driftsprocedurer, ændringsstyring, sikkerhedskopiering og overvågning

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*
- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*
- *At registrere hændelser og tilvejebringe bevis.*
- *At sikre integriteten af driftssystemer.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At minimere virkningen af auditaktiviteter på driftssystemer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Sikkerhedskopiering • GlobalConnect anvender tredjeparts leverandør (Frontsafe A/S) til al sikkerhedskopiering af driftssystemerne. • Frontsafe A/S har dokumenteret sine kontroller i en ISAE 3402 revisorerklæring, som GlobalConnect årligt gennemgår.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af Service Level Agreement fra Frontsafe A/S vedrørende Cloud Backup services. Vi har observeret, at serviceleverandøren har indhentet og gennemgået uafhængig revisors ISAE 3402-erklæring for perioden fra 1. oktober til 30. september 2018 vedrørende tekniske og organisatoriske sikringsforanstaltninger i tilknytning til driften af Cloud Backup-ydelser. Vi har foretaget inspektion af den ovenfor anførte ISAE 3402-erklæring.	Ingen afvigelser konstateret.
Ændringsstyring • GlobalConnect har etableret en proces for styring af ændringer i datacentre som foretages efter fastlagte rutiner for ændringsstyring. • Ændringer og styring heraf dokumenteres i Service Management System. • Kunder varsles efter et fastlagt tidsskema, forinden ændringsarbejdet, for at sikre mindst mulig gene for kunderne.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af procedure for implementering og drift af datacentre og procedure for ændringsstyring, herunder instrukser og tjeklister. Vi har observeret, at planlagte arbejder oprettes i Service Management System, og at OMC er ansvarlig for ændringsstyringen, herunder varsling af berørte kunder, opfølgning af igangsatte arbejder og dokumentation af udførte ændringer. Vi har foretaget inspektioner i Service Management System som dokumentation for vores observation.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed Driftsprocedurer, ændringsstyring, sikkerhedskopiering og overvågning		
Kontrolmål • *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.* • *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.* • *At registrere hændelser og tilvejebringe bevis.* • *At sikre integriteten af driftssystemer.* • *At forhindre, at tekniske sårbarheder udnyttes.* • *At minimere virkningen af auditaktiviteter på driftssystemer.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
	Vi har foretaget inspektion af oversigt over planlagte arbejder for perioden 1. januar til 30. april 2018, hvor disse blev styret i regneark. Vi har foretaget inspektion af udtræk fra Service Management System over planlagte arbejder for perioden 1. april til 31. december 2018. Vi har foretaget inspektion af dokumentation for stikprøvevis udvalgte planlagte arbejder og observeret ændringsstyringsprocessen, herunder varsling af kunder og færdiggørelse af arbejdet inden for den udmeldte tidsfrist.	
Hændelseslogning • Der er etableret registrering og håndtering af alle relevante hændelser. • Netværk overvåges med softwareværktøjer. Der er opsat alarmer, som notificerer ved netværksfejl. • Alle Datacentre overvåges af OMC, 24/7/365, og enhver begivenhed eller alarm undersøges med det samme. • Der åbnes en fejlrapport i Service Management System på alle fejl med et referencenummer, som benyttes gennem hele den efterfølgende fejlhåndteringsproces.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedurer for overvågning af datacenterløsninger, herunder procedurer og retningslinjer for hændelsesstyring, krisestyring ved kritiske fejl samt kriseberedskab. Vi har observeret, at overvågning i OMC sker både systemmæssigt og visuelt på skærme, og at de indført procedurer og retningslinjer følges, herunder registrering af hændelser. Vi har observeret, at hændelser registreres i Service Management System. Vi har foretaget inspektion af udtræk fra dette system over alle hændelser, der er indtruffet og oprettet i 2018 i kategorien Datacenterløsning.	Ingen afvigelser konstateret.

A.12: Driftssikkerhed
Driftsprocedurer, ændringsstyring, sikkerhedskopiering og overvågning

Kontrolmål

- *At sikre korrekt og sikker drift af informationsbehandlingsfaciliteter.*
- *At sikre, at information og informationsbehandlingsfaciliteter er beskyttet mod malware.*
- *At registrere hændelser og tilvejebringe bevis.*
- *At sikre integriteten af driftssystemer.*
- *At forhindre, at tekniske sårbarheder udnyttes.*
- *At minimere virkningen af auditaktiviteter på driftssystemer.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
	Vi har foretaget inspektion af stikprøvevis udvalgte hændelser i Service Management System med prioriteten kritisk eller høj, herunder observeret, at responstider overholdes. Vi har foretaget inspektion af procedure for eskalation ved kritiske fejl og observeret, at OMC følger proceduren. Vi har foretaget inspektion af månedsrapporter fra OMC.	

A.16: Styring af informationssikkerhedsbrud

Kontrolmål

- *At sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Håndtering af informationssikkerhedsbrud • Alle sikkerhedsbrud (security incidents) håndteres i Service Management System og i henhold til etablerede procedurer.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens informationssikkerhedspolitik og informationssikkerhedsregler samt procedurer for håndtering af sikkerhedsbrud, herunder procedurer og retningslinjer for eskalationsproces. krisestyring ved kritiske fejl og kriseberedskab. Vi har observeret, at hændelser registreres i Service Management System. Vi har foretaget inspektion af udtræk fra dette over alle hændelser, der er indtruffet og oprettet i 2018. Vi har foretaget inspektion af stikprøvevis udvalgte hændelser i Service Management System med prioriteten kritisk eller høj. Vi har foretaget inspektion af procedure for eskalation ved kritiske fejl og observeret, at OMC følger proceduren.	Ingen afvigelser konstateret.
Rapportering af informationssikkerhedshændelser • Der er etableret processer og procedurer for håndtering af sikkerhedshændelser for at sikre en ensartet og effektiv metode til styring af informationssikkerhedsbrud, herunder kommunikation om sikkerhedshændelser og -svagheder, som dokumenteres i Service Management System. • Der er etableret processer og procedurer, som sikrer, at sikkerhedshændelser registreres og håndteres af rette medarbejdere.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens procedurer og retningslinjer for hændelsesstyring, krisestyring ved kritiske fejl samt kriseberedskab. Vi har observeret, at hændelser registreres i Service Management System, og at styringen af hændelsen understøttes af dette system, herunder tildeling af sikkerhedshændelsen til rette medarbejder samt kommunikation og rapportering. Vi har foretaget inspektion af stikprøvevis udvalgte hændelser i Service Management System med prioriteten kritisk eller høj. Vi har observeret, at de indførte procedurer følges.	Ingen afvigelser konstateret.

A.17: Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring Informationssikkerhedskontinuitet og redundans

Kontrolmål

- *Informationssikkerhedskontinuiteten skal være forankret I organisationens ledelsessystemer for nød-, beredskabs- og retableringsstyring.*
- *At sikre tilgængelighed af informationsbehandlingsfaciliteter.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Implementering af informationssikkerhedskontinuitet • Der er udarbejdet beredskabsplaner for Datacentre, som sikrer forretningens videreførelse ved sikkerhedshændelser, som er gældende 5 år frem i tiden. • Beredskabsplanerne opdateres periodisk.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens overordnede risikovurdering og tilhørende beredskabsplaner og procedurer. Vi har desuden foretaget inspektion af procedure for OMC hændelsesstyring og procedure for krisestyring ved kritiske fejl og kriseberedskab. Vi har observeret, at serviceleverandøren løbende opdaterer beredskabsplanerne baseret på risikovurderinger, og at opdatering sker minimum hvert andet år. Vi har inspiceret, at beredskabsplanerne for Operations og Datacentre senest er opdateret i marts 2017, og at de er gældende frem til 2023.	Ingen afvigelser konstateret.
Verificering, gennemgang og evaluering af informationssikkerhedskontinuiteten • GlobalConnect har etableret periodisk afprøvning af beredskabsplaner med formålet at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer. • Beredskabstests dokumenteres ved rapporter fra øvelserne.	Vi har udført forespørgsel hos passende personale hos serviceleverandøren. Vi har foretaget inspektion af serviceleverandørens overordnede risikovurdering og tilhørende beredskabsplaner og procedurer, herunder procedurer for afprøvning af beredskabsplaner. Vi har foretaget inspektion af serviceleverandørens plan for afprøvning af beredskabsplanerne, der løber fra 2018 til 2023. Vi har observeret, at serviceleverandøren har udført den planlagte afprøvning af beredskabet i henhold til planen. Vi har foretaget inspektion af dokumentationen for afprøvningerne i form af udarbejdede rapporter, der refererer til registreringer i Service Management System. Vi har observeret, at der følges op på eventuelle bemærkninger eller forbedringsforslag i serviceleverandørens kvalitets- og sikkerhedsudvalg.	Ingen afvigelser konstateret.

BDO Statsautoriseret revisionsaktieselskab

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