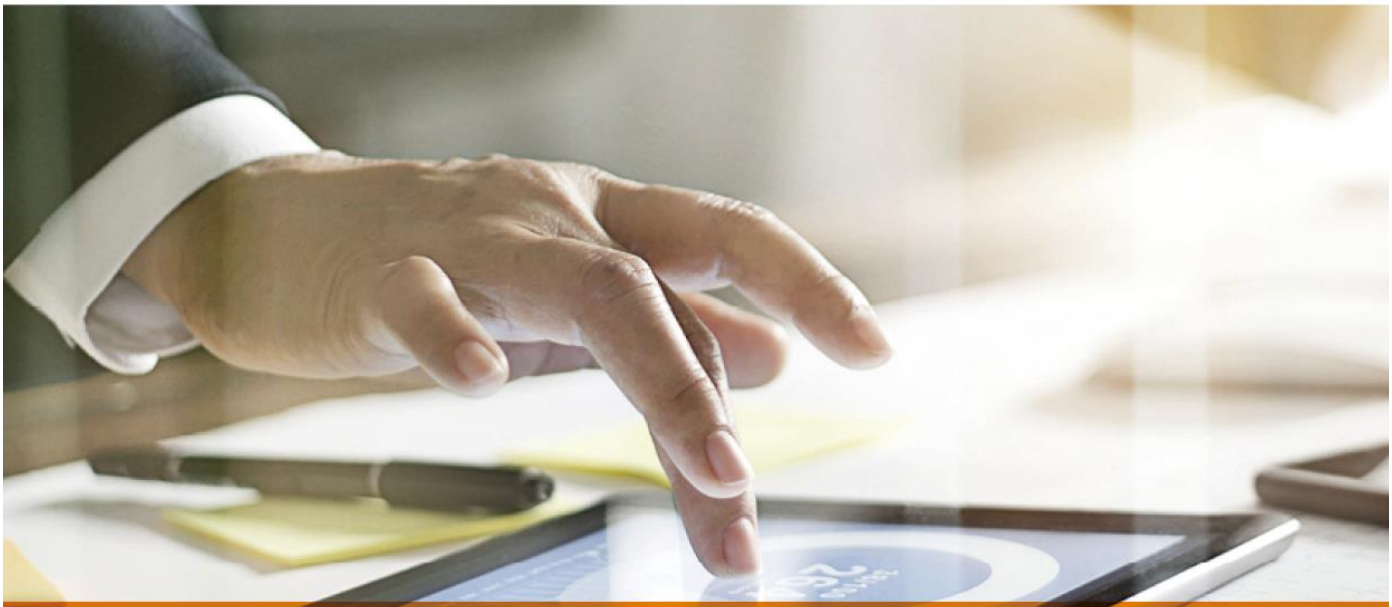
BEIERHOLM
VI SKABER BALANCE



JANUAR 2022

GlobalConnect A/S

ISAE 3402 TYPE 2 ERKLÆRING

Uafhængig revisors erklæring om kontrolmiljøet for it-driften i tilknytning til GlobalConnect Outsourcing Services.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

Erklæringsopbygning

Kapitel 1:
Ledelseserklæring.

Kapitel 2:
Beskrivelse af kontrolmiljøet for it-driften i tilknytning til GlobalConnect Outsourcing Services.

Kapitel 3:
Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet.

Kapitel 4:
Revisors beskrivelse af kontrolmål, sikkerhedstiltag, tests og resultater heraf.

KAPITEL 1:

Ledelseserklæring

GlobalConnect A/S har udarbejdet medfølgende beskrivelse af kontroller i tilknytning til GlobalConnect Outsourcing Services.

Medfølgende beskrivelse er udarbejdet til brug for kunder (og deres revisorer), der har anvendt GlobalConnect Outsourcing Services (herefter benævnt GlobalConnect), og som har en tilstrækkelig forståelse til at vurdere beskrivelsen sammen med anden information, herunder information om kontroller, som kunderne dvs. de dataansvarlige selv har udført, ved vurdering af, om kravene til kontrolmiljøet samt databeskyttelsesforordningen er overholdt.

GlobalConnect A/S anvender en serviceunderleverandør til sikkerhedskopiering. Denne serviceunderleve-randørs relevante kontrolmål og tilknyttede kontroller indgår ikke i den medfølgende beskrivelse (partielmetoden).

Datacenterafdelingen i GlobalConnect A/S er serviceunderleverandør i forhold til den fysiske sikkerhed i de datacentre, hvorfra GlobalConnect Outsourcing Services afvikles. Beskrivelsen indeholder ikke kontrol-mål og kontroller, der håndteres af Datacenterafdelingen, og omfatter således udelukkende kontrolmål og kontroller for processer og procedurer, som håndteres af GlobalConnect Outsourcing Services (partielmetoden).

GlobalConnect bekræfter, at:

(A) Den medfølgende beskrivelse, kapitel 2, giver en retvisende beskrivelse af GlobalConnect kontrolmiljø i tilknytning til driften af GlobalConnect Outsourcing Services i hele perioden 1. januar 2021 - 31. december 2021. Kriterierne for dette udsagn er, at den medfølgende beskrivelse:

(i) Redegør for, hvordan kontrollerne 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 styring af de generelle it-kontroller.
- De relevante kontrolmål og de kontrolaktiviteter, der er udformet til at nå disse mål.
- De kontroller, som vi med henvisning til udformning af vores services har forudsat ville være implementeret af kunden, og som, hvis det er nødvendigt for at nå de kontrolmål, der er anført i beskrivelsen, er identificeret i beskrivelsen sammen med de specifikke kontrolmål, som vi ikke selv kan nå.
- De andre aspekter ved kontrolmiljøet, risikovurderingsprocessen, informationssystemerne, kommunikationen, kontrolaktiviteterne og overvågningskontrollerne, som har været relevante for de leverede services.

(ii) Indeholder relevante oplysninger om ændringer i kontroller i tilknytning til GlobalConnect Outsourcing Services i hele perioden 1. januar 2021 - 31. december 2021.

(iii) Ikke udelader eller forvansker oplysninger, der er relevante for omfanget af de beskrevne kontroller under hensyntagen til, at beskrivelsen er udarbejdet for at opfylde de almindelige behov

hos en bred kreds af kunder og deres revisorer og derfor ikke kan omfatte ethvert aspekt ved kontroller, som den enkelte kunde måtte anse som vigtigt efter deres særlige forhold.

(B) De kontroller, der knytter sig til de kontrolmål, der er anført i medfølgende beskrivelse, var hensigtsmæssigt udformet og fungerede effektivt i hele perioden 1. januar 2021 - 31. december 2021. Kriterierne for dette udsagn er, at:

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

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

(iii) Kontrollerne var anvendt konsistent som udformet, herunder at manuelle kontroller blev udført af personer med passende kompetence og beføjelse i hele perioden 1. januar 2021 - 31. december 2021.

(C) Den medfølgende beskrivelse og de tilhørende kriterier for opnåelse af kontrolmål og kontroller, kapitel 2, er udarbejdet med baggrund i overholdelse af GlobalConnect A/S' standardaftale. Kriterierne for dette grundlag var:

(i) Service Level Agreement version 1.1
(ii) Databehandleraftale version 1.1.b

København, den 27. januar 2022.

GlobalConnect A/S

Louise Hahn

Country CEO DK & Germany

KAPITEL 2:

Beskrivelse af kontrolmiljøet for it-drift-ten i tilknytning til GlobalConnect

OVERORDNET BESKRIVELSE AF GLOBALCONNECT A/S

GlobalConnect A/S (GlobalConnect), del af Nordic Connectivity AB, er udbyder Sort Fiber løsninger, Transmissionsløsninger, Outsourcing Services, herunder cloud services, samt Datacenterløsninger i Danmark til bl.a. en række private og offentlige virksomheder.
Nærværende beskrivelse er udarbejdet med henblik på at rapportere om de generelle it-kontroller, som GlobalConnect Outsourcing Services (GCOS) anvender til at understøtte og sikre leverancen af it-drift til sine kunder. Beskrivelsen fokuserer på forretningsrelevante kontrolmål og processer, der er etableret med henblik på at sikre GCOS' leverance.
Datacenterafdelingen i GlobalConnect A/S er serviceunderleverandør i forhold til den fysiske sikkerhed i de datacentre, hvorfra GCOS ydelser afvikles. Nærværende beskrivelse indeholder ikke kontrolmål og kontroller, der håndteres af Datacenterafdelingen.

BESKRIVELSE AF GLOBALCONNECT OUTSOURCING SERVICES' YDELSER

GCOS har siden 2001 specialiseret sig i at levere it-outsourcing og it-drift til et bredt udsnit af offentlige og private virksomheder på det danske marked. Som mellemstor leverandør har GCOS formået at bibeholde et unikt fokus på at understøtte vores kunders evne til at drive en effektiv forretning i offentlig eller privat kontekst. Dette er vel at mærke uden, at det er gået ud over de helt fundamentale it-egenskaber: stabilitet, kost-effektivitet, skalerbarhed og ikke mindst leverancesikkerhed.

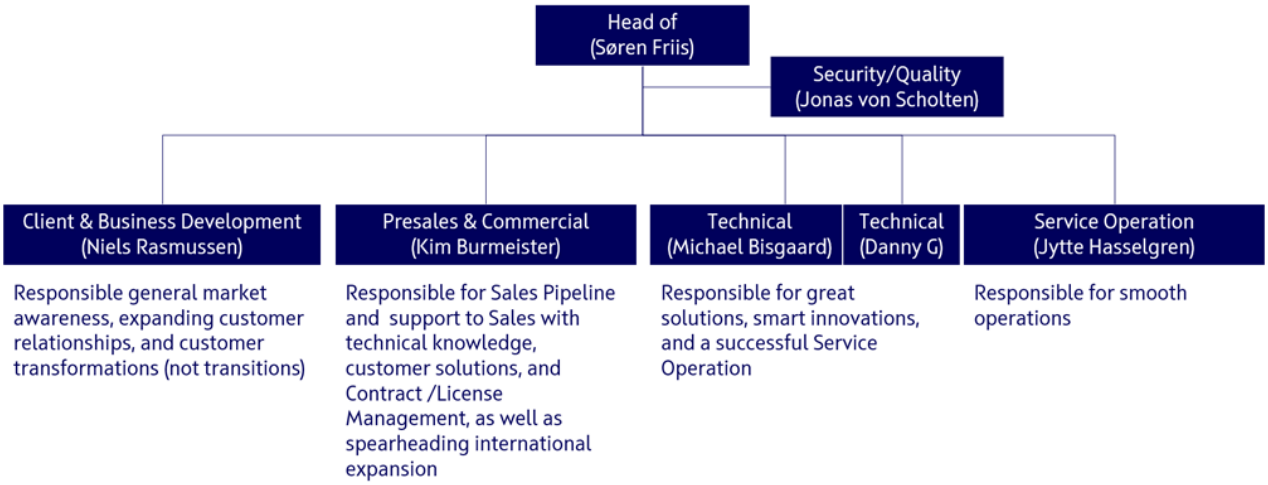
GCOS er vokset støt gennem årene. Dette skyldes ikke blot tilgang af nye kunder men i særdeleshed også fastholdelsen og udvidelse af eksisterende kundeforhold. Vi har således gennem alle årene haft et unikt fokus på kundetilfredshed gennem kvalitetssikring.

GCOS har etableret et kvalitetsledelsessystem med udgangspunkt i kravene i ISO 9001:2015, hvormed der kontinuerligt arbejdes med at højne kvaliteten i alle leverancer. Det betyder, at alle led af leverancekæden er kvalitetssikrede; lige fra valg af leverandører, over interne politikker for bl.a. personale, efterlevelse af alle relevante myndigheds- og lovkrav, til de helt centrale ITIL-funderede driftsprocesser. Det betyder endvidere, at alle forbedringsmuligheder løbende kortlægges; såvel dem, som vi selv identificerer, som dem vores kunder måtte identificere.

Som specialiseret sourcing og cloud -partner er vores fornemste opgave at levere stabil og sikker 24/7-drift og -vedligeholdelse, samt at sikre, at det sker i henhold til best practice på området. Dette betyder, at vi leverer på de aftalte service-levels (SLA'er og KPI'er), samt at forretningssamarbejdet med os aktivt bidrager til værdiskabelse og teknologiske udvikling hos vores kunder. Tilsvarende gælder det for vores kunder, at de får adgang til "kritisk masse" i form af vores kernekompetencer, dvs. teknologidrift, ekspertviden, processer og sikkerhed. Vores kunder kan derved frigøre ressourcer og koncentrere sig om deres kerne-forretning.

OVERORDNET BESKRIVELSE AF GLOBALCONNECT OUTSOURCING SERVICES' ORGANISATION

GCOS har flere højt certificerede partnerskaber med flere førende teknologileverandører, herunder Microsoft CSP Gold Partner, VMware VCPP (VMware Cloud Provider Program) og Dell Platinum Partner. GCOS' ansatte har relevante produkt- og teknologicertificeringer inden for de teknologier, som leveres til vores kunder. GCOS' medarbejdere er endvidere ITIL-certificerede. Nedenstående organisationsdiagram angiver GC-OS' formelle funktionsopdeling.



RISIKOSTYRING AF GLOBALCONNECT OUTSOURCING SERVICES

Der gennemføres periodisk risikovurderinger, dog minimum én gang om året 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.
Herudover vurderes og håndteres risici også helt naturligt på taktisk og operationelt niveau. I praksis er risikovurderinger et eksplicit element i adskillige af vores ITIL-baserede driftsprocesser, og vi registrerer potentielle sikkerhedsrelaterede hændelser forårsaget af såvel eksterne som interne forhold i vores Servicedesk-system til efterfølgende analyse.
Risikovurderinger tager udgangspunkt i implementeringsvejledningerne i den internationale standard ISO27005.
Sandsynlighed og konsekvens for truslerne (re)vurderes ud fra de informationer, der er til rådighed på det pågældende tidspunkt. Disse er tilsammen et udtryk for trusselsniveauet. 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.
GCOS har en formel proces for håndtering af risiko, som afleder konkrete handlingsplaner. Handlingsplanerne er allokeret og adresseret i henhold til proceduren for risikohåndtering. 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.
Denne erklæring inkluderer udelukkende kontroller og kontrolmål for processer og kontroller, som håndteres af GCOS, og indeholder således ikke kontroller og kontrolmål, der håndteres af underleverandører.

KONTROLRAMMER, KONTROLSTRUKTUR OG KRITERIER FOR KONTROLIMPLEMENTERING

GCOS' informationssikkerhed er defineret ud fra målsætningen om at levere dedikeret it-outsourcing og infrastrukturløsninger af højeste kvalitet, herunder stabilitet og sikkerhed.
Fastsættelse af kriterier og omfang for kontrolimplementering hos GCOS sker med udgangspunkt i ISO 27001:2013 – Annex A, refereret i ISO 27002, Regelsæt for styring af informationssikkerhed. Følgende kontrolområder i ISO 27001 – Annex A er evalueret:

- A.5. Informationssikkerhedspolitik

- A.6. Organisering af informationssikkerhed
- A.7. Personalesikkerhed
- A.8. Styring af aktiver
- A.9. Adgangsstyring
- A.10. Kryptografi
- A.11. Fysisk sikring og miljøsikring
- A.12. Driftssikkerhed
- A.13. Kommunikationssikkerhed
- A.14. Anskaffelse, udvikling og vedligehold af systemer
- A.15. Leverandørforhold
- A.16. Styring af informationssikkerhedsbrud
- A.17. Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring
- A.18. Overensstemmelse

Etableret kontrolmiljø
De etablerede kontroller er baseret på de administrative systemer, hvormed GCOS leverer ydelser til sine kunder og omfatter kontrolområder og kontrolaktiviteter for drifts- og hosting-leverancer. Hvert enkelt område ovenfor er detaljebeskrevet nedenfor i separate afsnit, og de beskrevne kontrolmål og kontroller for disse områder i afsnit om kontrolmål, kontroller, test og resultat af test er en integreret del af beskrivelsen.

A.5 Informationssikkerhedspolitik
GlobalConnect har etableret en formel informationssikkerhedspolitik. Den udleveres ved ansættelse, og herudover er alle medarbejdere også underlagt krav om, at de ajourfører sig periodisk i forhold informationssikkerhedspolitik med tilhørende underpolitikker, direktiver og instruktioner. GCOS har endvidere formuleret en mere specificeret politik, informationssikkerhedsreglerne, som kan tilgås af alle ansatte, med periodiske påmindelser om bekendtgørelse af reglernes formål og indhold.

A.6 Organisering af informationssikkerhed
GCOS 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 it-sikkerhedsledelsen i organisationen. Det formelle ansvar, herunder godkendelse af informationssikkerhedspolitikken og procedurer, ligger således også hos CEO, dog kan ansvaret herfor, eller dele heraf, uddelegeres til relevante ledelsesrepræsentanter for en specifik forretningsenhed.

Koordinering af informationssikkerheden
Aktiviteter til sikring af informationssikkerheden behandles i et tværfagligt Kvalitets- og Sikkerhedsudvalg (GCOS-QSF) med deltagelse fra alle relevante afdelinger. Endvidere koordineres aktiviteter og indsatser med det øvrige GlobalConnect.

Placering af informationssikkerhedsansvar
Alle ansvarsområder for it-sikkerheden er beskrevet i GCOS' sikkerhedspolitik, hvoraf der fremgår en klar ansvarsplacering i forbindelse med informationssikkerhed og beredskabsplanlægningen.

Mobil databehandling og -kommunikation
GCOS' politikker angiver retningslinjer for anvendelse af mobilt udstyr uden for virksomheden. Medarbejdere kan tilgå virksomhedens netværk og systemer eksternt, udelukkende gennem VPN eller "Jumphost" der er beskyttet med multifaktor autentificering.
Adgang fra hjemmearbejdsplads er sikret via krypterede VPN-forbindelse, eller fjernarbejdspladsmiljø som kræver validering via Active Directory understøttet af multifaktor autentificering.

Autentifikation af brugere på eksterne forbindelser
Enhver adgang til vores netværk, herunder for eksterne brugere, er autoriseret gennem vores formelle Access Management procedurer.

A.7 Personalesikkerhed
GlobalConnect har etableret kontroller, som sikrer, at ansatte er kvalificerede samt bevidste om deres opgaver og ansvar i relation til informationssikkerhed med tilhørende underpolitikker, direktiver og instruktioner.

I forbindelse med ansættelse i GCOS skal ansøgere aflevere en ren straffeattest, hvilket der endvidere følges op på ved forlangende. Operationelle medarbejdere med adgang til relevante kundedata skal tillige sikkerhedsgodkendes af PET/FE til minimum "Fortrolig".

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 'all-hands'-møder og dels på afdelingsmøder.

Roller og ansvar
Medarbejdernes ansvar følger deres placering i organisationen. Alle medarbejders ansvar i forhold til it-sikkerhed er beskrevet i organisationsplanen(reflekteret i organisationsdiagrammet), og hvor der er et udvidet ansvar, er dette beskrevet i sikkerhedspolitikken.

Fortrolighedserklæringer
Tavshedspligt og hemmeligholdelsesbestemmelser er en del af ansættelseskontrakterne.

Forpligtelser i forbindelse med fratrædelser
Generelle vilkår for ansættelse, herunder forhold omkring ophør, er beskrevet i medarbejderens ansættelses-kontrakt 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 igennem et workflow, forankret hos HR-afdelingen.

Nedlæggelse af adgangsrettigheder
GCOS' formelle HR procedurer sikrer, at alle rettigheder og fysiske adgange inddrages, når en ansættelse ophører. Dette sker det gennem et workflow, forankret i HR-afdelingen. Som en del af vores kvalitetsledelses-system gennemgås adgange mindst en gang i kvartalet.

Sanktioner i forbindelse med brud på sikkerhedspolitikken
I tillæg til almindelige ansættelsesretslige regler er sanktioner specificeret i personaleguiden. Arbejdspladsen er underlagt GCOS' sikkerhedsrutiner, som ikke må brydes. Sker dette, betragtes det som en misligholdelse af ansættelsesaftalen, og kan have ansættelsesmæssige konsekvenser.

A.8 Styring af aktiver
GCOS har etableret kontroller som sikrer at der opnås og vedligeholdes en passende beskyttelse af organisationens udstyr.

Registrering af udstyr
Relevant udstyr, der er taget i drift, registreres i GCOS' CMDB i servicedesk system, hvori enhver ændring også registreres.

Accepteret anvendelse af udstyr
Medarbejdernes anvendelse af it-udstyr og data er underlagt faste retningslinjer, defineret i GlobalConnect og GCOS' informationssikkerhedsinstruktioner, herunder men ikke begrænset til, politikker, direktiver og regler.

Styring af bærbare medier
Regler for anvendelsen af bærbare medier er indeholdt i klassifikationssystemet beskrevet i de generelle politikker for informationssikkerhed for GlobalConnect og i informationssikkerhedsreglerne gældende for GCOS.

Procedurer for informationshåndtering
Al behandling af data følger retningslinjer udstukket i klassifikationssystemet for GCOS.

A.9 Adgangsstyring
GCOS 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.

Procedure for adgangskontrol
Som supplement til vores sikkerhedspolitik har GC-OS en formel procedure for adgangsstyring (Acces Management).

Retningslinje for brug af netværksservices
Alle brugeres rettigheder, herunder adgang til netværk, drev og applikationer, er fastlagt ud fra deres funktion.

Brugeroprettelse
GCOS har procedurer for oprettelse og nedlæggelse af brugere, som er forankret i form af workflows i vores servicedesk system.

Udvidede rettigheder
Alle rettigheder er styret ud fra medarbejdernes roller og kontrolleres løbende under vores kvalitetsledelsessystem. Udvidelse af standardrettigheder følger vores formelle Access Management procedure.

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

Revurdering af brugeradgangsrettigheder
Alle adgange og rettigheder gennemgås periodisk af såvel den kvalitetsansvarlige som afdelingsledelsen.

Brugeridentifikation og autentifikation
GCOS har separate admin-profiler for alle driftsmedarbejdere på de systemer, hvor det er teknisk muligt. Al passwordvalidering foregår via systemer til håndtering af logininformationer, som håndterer validering for de individuelle logins.

A.10 Kryptografi
GCOS har etableret kontroller som sikrer korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

Datatrafik
Backupdata, der sendes over dedikerede linjer til underleverandøren, sikres med en eller flere krypteringsnøgler.

A.11 Fysisk sikring og miljøsikring
GCOS har etableret kontroller, som sikrer at it-udstyr er behørigt beskyttet mod uautoriseret fysisk adgang samt miljømæssige hændelser.

Fysisk adgangskontrol
GCOS' lokaler er forsynet med adgangskontrol i form af påkrævet personlig kode og personligt adgangskort for at sikre, at kun autoriseret personale får adgang. Kun GlobalConnects medarbejdere har udleveret personligt adgangskode. Såfremt leverandører, konsulenter eller andre eksterne skal have adgang, kan dette kun ske i følgeskab med autoriseret personale.

Sikring af kontorer, lokaler og faciliteter
GCOS' lokaler er forsynet med adgangskontrol i form af påkrævet personlig kode og personligt adgangskort for at sikre, at kun autoriseret personale får adgang.

Beskyttelse mod fysiske eksterne trusler
Der henvises til særskilt ISAE 3402-erklæring om beskrivelsen af kontroller, deres udformning og funktionalitet i tilknytning til GlobalConnects Datacenterløsning.

Opbevaring af udstyr og beskyttelse af udstyr
Det kritiske udstyr er placeret i serverrummet, som kun det tekniske personale har adgang til.

A.12 Driftssikkerhed
GCOS har etableret kontroller, som sikrer, at drift af servere og væsentlige systemer foregår på en struktureret og sikker måde.

Dokumenterede driftsprocedurer
Samtlige driftsprocedurer er indeholdt i GCOS' kvalitetsstyringssystem og er derfor lettilgængelige for alt personale gennem vores kvalitetsportal. De er alle funderet i ITIL og integreret i vores servicedesksystem. Kvalitetsledelsessystemet medfører vedligeholdelse og minimum et årligt review af samtlige procedurer.

Sikring af systemdokumentation
GCOS opbevarer systemdokumentationen centralt i vores Knowledge Database i servicedesk, som kun kan tilgås af autoriserede medarbejdere.

Kontrol af ændringsprocedurer
Vi har en formel procedure for ændringshåndtering, som er forankret i vores servicedesk system.

Styring af kapacitet
Der er etableret overvågning af kapacitet i forhold til internet, netværk, servere, diskplads og logfiler. GC-OS modtager rapportering fra N-able og andre værktøjer, som bruges i planlægning af indkøb af mere kapacitet. Data fra overvågning registreres og evalueres løbende.

Backup af information
Der tages backup af alle væsentlige data i henhold til indgåede kundeaftaler. Fejl i backup identificeres igennem backupværktøjet og registreres i GCOS' servicedesk. Restoretest for kunden udføres kun, når der foreligger en specifik aftale mellem kunden og GCOS.
Kontrol af ondsindet kode

Alle registrerede servere i GCOS' infrastruktur er opdateret med godkendt antivirus software i henhold til Best Practice inden for området. Ved opsætning af ny server sikres det igennem workflows i GCOS' servicedesk, at antivirus installeres. Alle arbejdsstationer i GCOS opdateres i henhold til Best Practice med antivirus-software. Nye arbejdsstationer installeres med et standardimage, der indeholder antivirus.

Audit log
Der foretages logning af brugertransaktioner, undtagelser og sikkerhedshændelser, og loggen opbevares i henhold til gældende politik eller i henhold til specifik aftale med kunden.

Brug af overvågningssystemer
GCOS har implementeret interne procedurer, som sikrer, at der bliver taget hånd om underretninger og alarmer med henblik på at reagere på relevante hændelser og handle derefter. Alle relevante alarmer vises på storskærm inden for normal arbejdstid og til den vagthavende i vagtperioderne. Alle alarmer gennemgås løbende af GCOS' driftsafdeling og bliver rapporteret til kunder i kraft af, at der oprettes sager på baggrund heraf.

Logning af administrator og operatør
Logning af systemadministratorers handlinger sker automatisk i vores servicedesk system og i de relevante logopsamlingssystemer for de konkrete systemer.

Logning af fejl
Det er opsat overvågning til fremtidig analyse af fejl og hændelser i vores servicedesk.

A.13 Kommunikationssikkerhed
GCOS har etableret kontroller, som sikrer, at drift af væsentlige infrastrukturkomponenter foregår på en struktureret og sikker måde.

Netværkskontroller
GCOS har nedskrevne procedurer for konfiguration af firewalls, routere og switche, som udelukkende foretages af driftsafdelingen.

Sikkerhedsydelser på netværket
Adgang til GCOS' systemer for vores kunder sker gennem offentlige netværk, hvor adgang sker gennem VPN, MPLS og firewall. Adgang og kommunikation mellem vores servere og internettet sker igennem vores centralt styrede firewall, hvor der er opsat logning. Al indgående netværkstrafik sker igennem vores firewalls. Kun godkendt netværkstrafik er tilladt igennem firewallen på baggrund af kunde request.

Politikker og procedurer for dataudveksling
Alle dataudvekslinger er som minimum krypterede, dvs. foregår over VPN eller SSL/TLS-kryptering.

Kontrol af netværksforbindelser
Kunders netværk begrænses af VLAN og Access-regler i vores Core router / firewall. Det er kun godkendt GCOS-personale, som kan tilgå de forskellige kunders VLANs via administrationsnettet (admin nettet) fysisk ved GCOS.

A.14 Anskaffelse, udvikling og vedligehold af systemer
GCOS har etableret kontroller, som sikrer, at servere og relevante infrastruktur komponenter opdateres og vedligeholdes i nødvendigt omfang, samt at dette foregår i en struktureret proces herfor.

Change management
GCOS har en formel Change Management procedure, som sikrer, at systemer revurderes og testes i forbindelse med større ændringer og følger processen i vores servicedesk system i form af formaliserede workflows. Sikkerhedsmæssige opdateringer (patches) foretages én gang om måneden i de servicevinduer, som er aftalt med kunderne. Alle andre servicepacks installeres udelukkende efter forespørgsel fra kunden eller efter godkendelse fra kunden som følge af anbefaling fra GCOS, og følger processen i vores servicedesk system i form af formaliserede workflows.

Kontrol af tekniske sårbarheder
Der scannes efter opdateringer til systemer ved hjælp af software værktøjer. Herefter følges GCOS' formelle procedure for patching.

A.15 Leverandørforhold
GCOS anvender flere leverandører i forbindelse med informationsbehandling, og disse administreres og evalueres i henhold til klassifikationerne af de services der leveres i forbindelse med en given informationsbehandling.

Håndtering af sikkerhed i aftaler med tredjemand
Såfremt der er tale om underleverandører, som er en integreret del af vores leverancer, fører vi tilsyn med leverandørens etablerede kontroller i form af indhentelse af ISAE 3402 revisorerklæring eller anden dokumentation ækvivalent hermed.

I tillæg hertil skal relevante leverandører og konsulenter underskrive en fortrolighedserklæring og tilkendegive, at de er bekendt med vores sikkerhedspolitik.

I det omfang GCOS' underleverandører opbevarer eller på anden vis håndterer persondata på vegne af GCOS' kunder under levering af underleverandørens ydelse til GCOS, handler underleverandøren som databehandler alene efter instruks fra GCOS og GCOS' kunde. Hermed forpligter GCOS's underleverandører sig til at træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at personoplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med databeskyttelseslovgivningen.

A.16 Styring af informationssikkerhedsbrud
GCOS har etableret kontroller, som sikrer, at sikkerhedshændelser håndteres rettidigt samt at der følges op på disse.

Alle hændelser, herunder sikkerhedshændelser, følger vores formelle Incident/Problem Management eller Request Fullfillment procedure. Disse er indeholdt i vores kvalitetsledelsessystem og forankret i vores servicedesk-system.

Processen indeholder bl.a. modtagelse og registrering, vurdering og visitering, evt. eskalation samt fejlsøgning og genetablering af alle hændelser. Alle prioritet 1-hændelser rapporteres direkte til vores driftschef, projektledere og øvrige relevante ledere. Dette sker automatisk i vores servicedesk-system. Herudover har vi indeholdt i vores kvalitetsledelsessystem en formel procedure for eskalation af alle typer hændelser, herunder sikkerhedshændelser.

A.17 Informationssikkerhedsaspekter ved nød-, beredskabs- og retableringsstyring
GCOS har udarbejdet en beredskabsplan og denne opdateres i nødvendigt omfang.

Informationssikkerhed integreret i beredskabsplanen
GCOS har en formel beredskabsplan, hvori informationssikkerhed er indarbejdet.
Udvikling og implementering af beredskabsplaner, der medtager informationssikkerhed

Vi har udviklet beredskabsplaner med henblik på at opretholde eller genskabe drift og sikre adgangen til data på det krævede niveau og inden for den acceptable tid efter nedbrud eller udfald af kritiske forretningsprocesser.

Ansvar og retningslinjer
Roller og ansvar er defineret i beredskabsplanen. Beredskabsledelsen har ansvaret for forskellige områder som beskrevet i beredskabsplanen.

Beredskabsplan
GCOS foretager løbende en vurdering af risici, og mindst én gang årligt i forbindelse med ledelsens review og godkendelse af sikkerhedspolitikken opdateres beredskabsplanen så den modsvarer det gældende risikobillede.

Afprøvning, vedligeholdelse og revurdering af beredskabsplaner
Beredskabsplanen testes en gang årligt for at sikre, at den er anvendelig, tilstrækkelig og effektiv.

A.18 Overensstemmelse med kundekrav samt lov- og myndighedskrav
GCOS har etableret kontroller, som sikrer, at alle relevante kundekrav samt lov- og myndighedskrav overholdes.

Compliance
Som led i kundernes idriftsættelse i GCOS er der etableret procedurer, som sikrer, at alle kundekrav er identificeret og adresseret. Således anvendes projektledelse til styring af kundernes implementering i GCOS' drifts-miljø.

Uafhængig vurdering af informationssikkerheden
En stor del af procedurerne og de underliggende kontroller er en del af vores ISO 9001 certificerede kvalitetsledelsessystem, som udover jævnlige interne audits ligeledes er underlagt årlig ekstern revision.

Endelig er GCOS ISO27001 certificeret inden for informationssikkerhed. Som en del heraf er der udarbejdet procedurer for årlig revurdering og godkendelse af underliggende politikker, proces- og procedurebeskrivelser, ligesom dette auditeres hvert år.

Privatlivets fred og beskyttelse af personoplysninger
GCOS opbevarer og behandler personoplysninger efter kundens instruks for de kunder, der har indgået databehandleraftaler med os (der henvises til vores separate ISAE 3000 erklæring på området).

FORETAGNE ÆNDRINGER I SERVICEYDELSER OG TILHØRENDE KONTROLLER

I perioden fra 1. januar til 31. december 2021 er der ikke foretaget væsentlige ændringer i Global-Connects serviceydelser og tilhørende kontroller inden for Outsourcing Services.

SUPPLERENDE INFORMATION OMKRING DET ETABLEREDE KONTROLMILJØ

Forhold, som skal iagttages af kundernes revisorer

For at opnå de ovenstående specificerede kontrolmål skal følgende kontroller være etableret og korrekt håndteret af brugerorganisationerne:

Brugeradministration

GCOS tildeler adgang til interne medarbejdere og håndtere brugeradministrationen. GCOS udfører også brugeradministration af kunders medarbejdere, hvis der er indgået en aftale om dette. Brugeradministrationen foregår efter anmodning fra kunden. Det er kundens ansvar er at sikre, at der tilgår GCOS de korrekte oplysninger vedrørende brugeradministrationen.

Konfiguration af sikkerhed
GCOS har etableret sikkerhed på netværkslaget i form af segmentering, krav til kodeord og logning. Hvis sikkerheden på kundernes servere ikke er konfigureret af GCOS, er kunderne selv ansvarlig for sikring af sikkerheden på servere, som hostes hos GCOS. Når GCOS installerer servere, benyttes en baseline, som sikrer en tilpas sikkerhed på serverne.

Disaster recovery
GCOS har etableret kontroller til sikring af, at data sikkerhedskopieres, og at sikkerhedskopiernes læsbarhed løbende kontrolleres, såfremt der er indgået en aftale herom med kunden. Hvis hele systemer skal reetableres, sikrer GCOS, at der er sikkerhedskopier af data tilgængelig til reetableringen, hvor GCOS´ kunder selv er ansvarlig for reetablering af systemerne. Hvis hele systemer skal reetableres, og der er indgået en aftale om dette, sørger GCOS for at dette kan lade sig gøre og tester dette i henhold til aftalen. GCOS' kunder er ansvarlige for at backup schedules og data retention planer, for systemer hvoraf der tages backup, er tilstrækkelige i forhold til kundernes individuelle forretningsbehov.

Beskyttelse af udstyr hos GCOS´ kunder
GCOS har etableret kontroller til fysisk beskyttelse af udstyr placeret hos GCOS, herunder udstyr placeret i GCOS´ datacenter. Beskyttelse af udstyret omfatter blandt andet begrænsning af den fysiske adgang til det relevante udstyr. GCOS' kunder er ansvarlig for fysisk sikring af udstyr placeret i eget fysisk miljø.

KAPITEL 3:

Uafhængig revisors erklæring med sikkerhed om beskrivelsen af kontroller, deres udformning og funktionalitet

Til kunder af GlobalConnect A/S og deres revisorer

Omfang

Vi har fået som opgave at afgive erklæring om GlobalConnect Outsourcing Services beskrivelse i kapitel 2, som er en beskrivelse af kontrolmiljøet i forbindelse med it-driften af GlobalConnect i perioden 1. januar 2021 - 31. december 2021, og om udformningen og funktionen af kontroller, der knytter sig til de kontrolmål, som er anført i beskrivelsen.

Vores konklusion udtrykkes med høj grad af sikkerhed.

Erklæringen er afgivet efter den partielle metode, hvilket betyder, at denne erklæring ikke omfatter de it-sikkerhedsmæssige kontroller og kontrolaktiviteter, som er tilknyttet i forbindelse med anvendelse af eksterne samarbejdspartnere. Erklæringen dækker ikke kontrol eller tilsyn med underleverandører i tilknytning til driften af Outsourcing Serviceaktiviteter. Disse underleverandører er nærmere oplistet i databehandleraftaler med kunderne.

Erklæringen dækker ikke kundespecifikke forhold. Desuden dækker erklæringen ikke de komplementerende kontroller og kontrolaktiviteter, som udføres af brugervirksomheden, jf. virksomhedsbeskrivelsen i kapitel 2, afsnittet om komplementerende kontroller hos kunderne.

GlobalConnect' ansvar

GlobalConnect Outsourcing Services er ansvarlig for udarbejdelsen af beskrivelsen og tilhørende udsagn i kapitel 2, herunder fuldstændigheden, nøjagtigheden og måden, hvorpå beskrivelsen og udsagnet er præsenteret; for leveringen af de ydelser, beskrivelsen omfatter, for at anføre kontrolmålene samt for udformningen, implementeringen og effektivt fungerende kontroller for at nå de anførte kontrolmål.

Beierholms uafhængighed og kvalitetsstyring

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

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

Revisors ansvar

Vores ansvar er, på grundlag af vores handlinger, at udtrykke en konklusion om GlobalConnect' beskrivelse samt om udformningen og funktionen af kontroller, der knytter sig til kontrolmål, der er anført i denne beskrivelse. Vi har udført vores arbejde i overensstemmelse med ISAE 3402, Erklæringer med sikkerhed om kontroller hos en serviceleverandør, som er udstedt af IAASB. Denne standard kræver, at vi overholder etiske krav samt 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 beskrivelse, udformning og funktionalitet 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 i de heri anførte mål samt hensigtsmæssigheden af de kriterier, som GlobalConnect har specificeret og beskrevet i kapitel 2.

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

Begrænsninger i kontroller hos GlobalConnect

GlobalConnect' 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 ved systemet, som hver enkelt kunde måtte anse for vigtig efter deres særlige forhold. Endvidere vil kontroller hos GlobalConnect, som følge af deres art, muligvis ikke forhindre eller opdage alle fejl eller udeladelser ved behandlingen eller rapporteringen af transaktioner. Herudover er fremskrivningen af enhver vurdering af funktionaliteten til fremtidige perioder undergivet risikoen for, at kontroller hos serviceleverandøren 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 kriterier, der er beskrevet i kapitel 1 i ledelsens erklæring. Det er vores opfattelse,

a) at beskrivelsen af GlobalConnect' kontrolmiljø i tilknytning til driften af GlobalConnect Outsourcing Services, således som det var udformet og implementeret i hele perioden 1. januar 2021 - 31. december 2021, i alle væsentlige henseender er retvisende, og

b) at kontrollerne, som knyttede sig til de kontrolmål, der er anført i beskrivelsen, i alle væsentlige henseender var hensigtsmæssigt udformet i hele perioden 1. januar 2021- 31. december 2021, 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 1. januar 2021 - 31. december 2021.

Beskrivelse af testede kontroller

De specifikke kontroller, der er testet, samt arten, den tidsmæssige placering og resultater af disse tests fremgår af kapitel 4.

Tiltænkte brugere og formål

Denne erklæring og beskrivelsen af test af kontroller under kapital 4 er udelukkende tiltænkt Global-Connect' kunder og deres revisorer, som har en tilstrækkelig forståelse til at overveje dem sammen med anden information, herunder information om kunders egne kontroller, når de vurderer om kravene til kontrolmiljøet er overholdt.

Søborg, den 28. januar 2022

Beierholm
Statsautoriseret Revisionspartnerselskab

Kim Larsen
Statsautoriseret revisor

Poul Halkjær Nielsen
Rådgiver, CISA

KAPITEL 4:

Revisors beskrivelse af kontrolmål, sikkerhedstiltag, test og resultater heraf

Vi har struktureret vores arbejde i overensstemmelse med ISAE 3402 – erklæring med sikkerhed om kontroller hos en serviceleverandør. For hvert kontrolmål indleder vi med et kort resumé af kontrolmålet, som det er beskrevet i referencerammen ISO27001 og 2, version 2017.

Hvad angår periode har vi i vores test forholdt os til, om GLOBALCONNECT A/S har levet op til kontrolmålene i perioden 1. januar 2021 - 31. december 2021.

Under det grå felt er tre kolonner:

- Første kolonne viser de aktiviteter, som GlobalConnect A/S jf. sin dokumentation har iværksat for at leve op til kravene.
- Anden kolonne viser, hvordan vi har valgt at teste, om det forholder sig som beskrevet.
- Tredje kolonne viser resultatet af vores test.

De udførte tests

De udførte tests i forbindelse med fastlæggelsen af kontrollers design, implementering og operationelle effektivitet er foretaget ved metoderne beskrevet nedenfor.

Inspektion	Gennemlæsning af dokumenter og rapporter, som indeholder angivelse omkring udførelse af kontrollen. Dette omfatter bl.a. gennemlæsning af og stillingtagen til rapporter og anden dokumentation for at vurdere, om specifikke kontroller er designet, så de kan forventes at blive effektive, hvis de implementeres. Endvidere vurderes det, om kontroller overvåges og kontrolleres tilstrækkeligt og med passende intervaller.
Forespørgsler	Forespørgsel til passende personale hos GlobalConnect. Forespørgsler har omfattet, hvordan kontroller udføres.
Observation	Vi har observeret kontrollens udførelse.
Genudføre kontrollen	Gentaget den relevante kontrol. Vi har gentaget udførelsen af kontrollen med henblik på at verificere, at kontrollen fungerer som forudsat.

KONTROLMÅL - INDLEDNING:

Risikovurdering og – håndtering

Risikovurdering skal identificere og prioritere risici med udgangspunkt i driften af GlobalConnect. Resultatet skal bidrage til at fastlægge og prioritere de nødvendige ledelsesindgreb og sikringsforanstaltninger for at imødegå relevante risici.

GlobalConnect kontroller	Revisors test af kontroller	Resultat af test
Der foretages en årlig risikovurdering, som forelægges og vurderes af ledelsen. Risikovurderingen indgår som en del af arbejdet med GlobalConnects informationssikkerhedsledelsessystem (ISMS).	Vi har forespurgt og indhentet det relevante materiale ifm. revisionen af risikohåndteringen. Vi har kontrolleret, at der for GlobalConnect arbejdes med en løbende vurdering af de risici, som opstår som følge af de forretningsmæssige forhold og deres udvikling. Vi har kontrolleret, at risiko er en integraldel af forretningens daglige arbejdsgange.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 5:

Informationssikkerhedspolitikker

Ledelsen skal udarbejde en informationssikkerhedspolitik, som bl.a. skal indeholde ledelsens sikkerhedsmålsætning, -politik og overordnede handlingsplan. Informationssikkerhedspolitikken vedligeholdes under hensyn til den aktuelle risikovurdering.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Ledelsen fastlægger og godkender politikker for informationssikkerhed, som efter godkendelse offentliggøres og kommunikeres til medarbejdere og relevante eksterne parter. Politikken revurderes iht. planlagte intervaller.	Vi har indhentet og gransket GlobalConnects seneste it-sikkerhedspolitik. Gennem revisionen har vi kontrolleret, at der sker løbende vedligeholdelse af it-sikkerhedspolitikken. Vi har kontrolleret, at politikken er godkendt inden for rammerne af GlobalConnects governancestruktur på området og at den er gjort tilgængelig for medarbejderne via GlobalConnects intranet.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har implementeret et årshjul, der sikrer en periodisk gennemgang af informationssikkerhedspolitikken	Der er foretaget interview med relevant ledelse og personale.Der er indhentet dokumentation, der understøtter kontrolaktiviteten.Der er på Group niveau besluttet et årshjul, der skal følges.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er formuleret en skriftlig informationssikkerhedspolitik, som revurderes årligt.	Der er foretaget interview med relevant ledelse og personale, og der er indhentet dokumentation. Der er på Group niveau besluttet et årshjul, der skal følges.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Informationssikkerhedspolitikken er opdateret og godkendt af ledelsen.	Gennem revisionen har vi inspiceret ispolitikken. Vi har kontrolleret, at politikken er godkendt inden for rammerne af GlobalConnects governancestruktur på området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 6:

Organisering af informationssikkerhed

Der skal etableres en styring af it-sikkerheden i virksomheden. Der skal være placeret et organisatorisk ansvar for it-sikkerheden med passende forretningsgange og instrukser. Den it-sikkerhedsansvarliges rolle skal bl.a. sikre overholdelse af sikringsforanstaltninger, herunder løbende ajourføring af den overordnede risikovurdering.

Virksomheden skal sikre, at fjernarbejdspladser og brugen af mobilt udstyr får et passende beskyttelsesniveau.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Ansvaret for informationssikkerheden i GlobalConnect er forankret i ledelsen.	Der er foretaget interview med relevant ledelse og personale. Der er indhentet dokumentation, der understøtter kontrolaktiviteten. Det fremgår tydeligt at det er et ledelsesansvar i Group beslutningerne for ISO-arbejdet. Ligeledes er det af GC og GCOS daglig ledelse bekræftet på møderne samt ved deres aktive deltagelse i de respektive sikkerhedsfora for GC og GCOS.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen har nedsat en tværorganisatorisk Kvalitets- og Sikkerhedsudvalg, der behandler aktiviteter til sikring af informationssikkerheden	Der er foretaget interview med relevant ledelse og personale. Der er indhentet dokumentation, der understøtter kontrolaktiviteten.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ledelsen har udpeget en Kvalitets- og Sikkerhedschef, der er overordnet ansvarlig for håndtering af informationssikkerhed	Der er foretaget interview med relevant ledelse og personale. Interview med DK-ledelsen samt Group CISO har bekræftet rollens betydning og eksistens.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Alle mobile enheder, som anvendes i arbejdsmæssig sammenhæng, skal have installeret og opdateret anti-virus.	Der er foretaget interview med relevant ledelse og personale. Det tekniske setup, der sikrer overholdelsen af kontrolaktiviteten, er vist og forklaret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Forbindelse til interne enheder skal foregå via to faktor autentifikation (SMS Passcode eller Direct Access).	Der er foretaget interview med relevant personale. Det tekniske setup, der sikrer overholdelsen af kontrolaktiviteten, er vist og forklaret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Alle eksterne enheder der forbinder sig til GlobalConnects interne netværk skal være omfattet af 2-faktor løsninger	Der er foretaget interview med relevant ledelse og personale. Det tekniske setup, der sikrer overholdelsen af kontrolaktiviteten, er vist og forklaret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 7:

Medarbejdersikkerhed

Det skal sikres, at alle nye medarbejdere er opmærksomme på deres særlige ansvar og rolle i forbindelse med virksomhedens informationssikkerhed for derigennem at minimere risikoen for menneskelige fejl, tyveri, svindel og misbrug af virksomhedens informationsaktiver.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Der foretages et baggrundstjek af alle jobkandidaters baggrund i overensstemmelse med forretningsmæssige krav og den funktion, som medarbejderen skal bestride.	Vi har interviewet relevant personale hos GlobalConnect. Vi har inspiceret arbejdsgangene for ansættelse. Straffeattest er default samt eventuel sikkerhedsgodkendelse beror på ansættende leders bestilling.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Ansættelse i GlobalConnect fordrer altid, at der kan fremvises en "straffeattest".	Vi har interviewet relevant personale hos GlobalConnect. Vi har inspiceret arbejdsgangen i det enedelsystem, der anvendes og set at punktet tydeligt fremgår af ansættelsesfanen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Når kunden eller arbejdsopgaven kræver sikkerhedsgodkendelse, indhentes sådanne for relevante medarbejdere i henhold til fastlagt procedure herfor.	Vi har interviewet relevant personale hos GlobalConnect. Vi har set at det overordnede flowdiagram fremgår det at sikkerhedsgodkendelse har sin egen underproces.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Medarbejdere i GlobalConnect informeres løbende om informationssikkerhedsmæssige forhold og evt. trusler i forhold til deres opgaver.	Vi har interviewet relevant personale hos GlobalConnect. Vi har modtaget eksempler på både awareness kampagner, NDAer samt set at emnet er behandlet på medarbejder fælles møder samt er rapporteret til ledelsen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Medarbejdere i GlobalConnect tilkendegiver ved ansættelsen, at de har læst og accepteret Informationssikkerhedspolitikken og -håndbogen	Vi har interviewet relevant personale hos GlobalConnect. Vi er blevet oplyst at man ved accept af ansættelsen skal underskrive at man har accepteret Informationssikkerhedspolitikken og -håndbogen. Disse er bilag ved fremsendelsen af kontrakten.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Alle medarbejdere, der arbejder med fortrolige data - herunder persondata - har underskrevet en fortrolighedserklæring.	Vi har interviewet relevant personale hos GlobalConnect. Vi er blevet oplyst at man ved accept af	Vi har ikke ved vores test konstateret væsentlige afvigelser.

	ansættelsen skal underskrive en NDA og er blevet forelagt eksempler på en NDA.	
Efter ansættelsesforholdets ophør eller ændring inddrages eller ændres adgange og rettigheder i forhold til det funktionsmæssige behov herfor.	Vi har interviewet relevant personale hos GlobalConnect. Vi har inspiceret arbejdsgangen og set dokumentation for dens udførelse. IT foretager nedtagning af rettigheder og vedligeholder Asset Registret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Efter ansættelsesforholdets ophør afleveres udleveret udstyr fra den fratrædende medarbejder	Vi har interviewet relevant personale hos GlobalConnect. Vi har inspiceret arbejdsgangen og set dokumentation for den udførelse på stikprøvebasis. IT foretager nedtagning af rettigheder og vedligeholder Asset Registret.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Efter ansættelsens ophør sikrer HR, at procedure for fratrædelse bliver overholdt	Vi har interviewet relevant personale hos GlobalConnect. Vi har inspiceret arbejdsgangen og set dokumentation for den udførelse på stikprøvebasis.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 8:

Styring af aktiver

Der skal være sikring og vedligeholdelse af den nødvendige beskyttelse af virksomhedens informationsaktiver, og alle virksomhedens fysiske og informationsrelaterede aktiver skal identificeres, og der skal udpeges en ansvarlig "ejer". Virksomheden skal sikre, at informationsaktiver i forhold til GlobalConnect får et passende beskyttelsesniveau.

Der skal være betryggende kontroller, som sikrer, at datamedier bliver bortskaffet på forsvarlig vis, når der ikke længere er brug for dem, i overensstemmelse med formelle procedurer.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Alt udstyr, der er relevant for leverance af ydelser, er identificeret og registreret i CMDB-systemet, hvori ændringer også registreres.	Vi har gennemgået registreringer i virksomhedens it-register i tilknytning til driften af GlobalConnect. Vi er oplyst at alt relevant udstyr registreres i CMDB.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret ejerskab for alt it-udstyr for alle kunder.	Vi har gennemgået registreringer i virksomhedens it-register i tilknytning til driften af GlobalConnect. Vi har observeret at der er registreret en ejer for aktiverne i CMDBen.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er udarbejdet retningslinjer for klassifikation af informationer og data. Al behandling af medier og data foretages i henhold til GlobalConnects klassifikationssystem.	Vi har interviewet relevant personale hos GlobalConnect. Vi har inspiceret dokumentation i form af guidelines.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 9:

Adgangsstyring

At styre adgangen til virksomhedens systemer, informationer og netværk med udgangspunkt i de forretnings- og lovgivningsbetingede krav. At sikre autoriserede brugeres adgang og forhindre uautoriseret adgang.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Der er vedtaget processer og procedurer for at styre adgange og begrænsninger til systemer og data på grundlag af forretnings- og funktionsmæssige behov	Vi har interviewet relevant personale hos GlobalConnect. HR føder de grundlæggende adgangskrav med ledergodkendelse. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Alle adgange og ændringer til adgange til systemer og data følger de vedtagne processer og procedurer	Vi har interviewet relevant personale hos GlobalConnect. HR føder de grundlæggende adgangskrav med ledergodkendelse. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect tildeler adgang til netværk og netværkstjenester efter "need-to-know" princippet	Vi har interviewet relevant personale hos GlobalConnect. HR føder de grundlæggende adgangskrav med ledergodkendelse. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har etableret og følger processen for oprettelse og afmelding af brugere i systemer	Vi har interviewet relevant personale hos GlobalConnect. HR føder de grundlæggende adgangskrav med ledergodkendelse. Det er af de adgangsgivende funktioner tydeligt understreget at der ikke sker oprettelser og nedlæggelser uden at de kommer ad de aftalte veje og med rette autorisationer. Der er forevist eksempler på afviste oprettelser.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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 interviewet relevant personale hos GlobalConnect. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

GlobalConnect har etableret en proces for nedlæggelse eller justering af adgangsrettigheder, herunder sletning af medarbejders adgang ved flytning eller fratrædelse	Vi har interviewet relevant personale hos GlobalConnect. Der er etableret en proces for nedlæggelse eller justering af adgangsrettigheder, herunder sletning af medarbejders adgang ved flytning eller fratrædelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har etableret tildeling af administrativ adgang til enheder i forhold til det funktionsmæssige behov som ligeledes er autoriseret	Vi har interviewet relevant personale hos GlobalConnect. Der er etableret en proces for tildeling af adgangsrettigheder, herunder tildeling og overvågning af administrative rettigheder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har etableret logning af adgange med privilegerede konti (administrative rettigheder)	Vi har interviewet relevant personale hos GlobalConnect. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har etableret proces og regler for tildeling og styring af adgangskoder	Vi har interviewet relevant personale hos GlobalConnect. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har etableret regler til etablering af adgangskoder, som skal følges af alle medarbejdere samt midlertidigt ansatte konsulenter	Vi har interviewet relevant personale hos GlobalConnect. Sikkerhedsmodellen og dens implementering er gennemgået.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 10:

Kryptografi

Det skal sikres at der sker korrekt og effektiv brug af kryptografi for at beskytte informationers fortrolighed, autenticitet og/eller integritet.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Der er udarbejdet processer og procedurer for oprettelse og vedligeholdelse af krypteringsnøgler hos de kunder, der har specificeret kravet i deres kontrakt med GlobalConnect	Vi har interviewet relevant personale hos GlobalConnect og har modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Backup-data transmitteres over dedikerede linjer til underleverandøren og sikres med en eller flere krypteringsnøgler	Vi har interviewet relevant personale hos GlobalConnect og har modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 11:

Fysisk sikkerhed og miljøsikring

Der skal være beskyttelse af virksomhedens lokaler og informationsaktiver mod uautoriseret fysisk adgang samt fysiske skader og forstyrrelser. Der skal opbygges sikkerhedstiltag, som sikrer, at der undgås tab af, skader på eller kompromittering af virksomhedens informationsaktiver samt forstyrrelser af virksomhedens forretningsaktiviteter. Beskyttelsesforanstaltningerne skal også omfatte sikring af nødvendige forsyninger som el, vand og ventilation samt kabelinstallationer.

GlobalConnect kontroller	Revisors test af kontroller	Resultat af test
Den etablerede fysiske perimetersikring er i overensstemmelse med de vedtagne sikkerhedskrav	Vi har gennemgået og kontrolleret, at datacentrene overholder de af ledelsen fastsatte krav. Herunder sikring mod: • brand • vandskade • strømafbrydelse • kølingssvigt • tyveri eller hærværk Konkret har vi: • påset tilstedeværelse af brandbekæmpelsessystemer og køling i datacenter. • gennemgået og kontrolleret dokumentation for vedligeholdelse til bekræftelse af, at UPS og dieselgenerator løbende vedligeholdes og testes. • observeret under besøg i datacenter, at der foretages monitering af UPS og dieselgenerator. • påset tilstedeværelse af udstyr til overvågning af indeklima i datacentre. • påset sikring af kabler for datakommunikation og elforsyning. • påset at der er indbrudsalarmer monteret relevant. • stikprøvevist gennemgået dokumentationen for, at vedligeholdelse af udstyr til beskyttelse mod fysiske trusler sker løbende.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret adgangskontroller, som forebygger sandsynligheden for uautoriseret fysisk adgang til, beskadigelse	Vi har interviewet relevant personale hos GlobalConnect. Der er foretaget on-site inspektion.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

og forstyrrelse af Global-Connects lokaler og informationer, herunder sikring af, at kun autoriserede personer har adgang	Der er et godkendelsesflow og brug af ADK til at sikre adgang.	
Aktiviteter registreres i adgangskontrolsystemet i OMC	Vi har interviewet relevant personale hos GlobalConnect. Der er foretaget on-site inspektion samt i OMCen. Der er observeret at der er adgangskontrol til stede både i kontorerne, til datacentre samt repeatersites.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Halvårlig gennemgang af eksterne adgangskort, der ikke har været i brug indenfor de seneste 6 måneder, er udført	Vi har interviewet relevant personale hos GlobalConnect. Vi har udtaget stikprøver der viser overholdelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Halvårlig gennemgang af interne adgangskort, der ikke har været i brug indenfor de seneste 6 måneder, er udført	Vi har interviewet relevant personale hos GlobalConnect. Vi har udtaget stikprøver der viser overholdelse.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Stikprøvekontrol af udvalgte adgangspunkter i forhold til, om rette personer har rette adgange	Vi har interviewet relevant personale hos GlobalConnect. Ledelsen autoriserer adgang igennem et procedure-understøttet workflow. Der er fremvist dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 12:

Driftssikkerhed

Kontrolmål: Driftsprocedurer og ansvarsområder

En korrekt og betryggende driftsafvikling af virksomhedens styresystemer skal sikres. Risikoen for teknisk betingede nedbrud skal minimeres. En vis grad af langtidsplanlægning er påkrævet for at sikre tilstrækkelig kapacitet. Der skal derfor foretages en løbende kapacitetsfremskrivning baseret på de forretningsmæssige forventninger til vækst og nye aktiviteter og de heraf afledte kapacitetskrav.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
GlobalConnect har etableret formelle driftsprocedurer som er tilgængelige for alle brugere som har et funktionsmæssigt behov for indsigt	Vi har interviewet relevant personale hos GlobalConnect. Der er generelt stillet driftsprocedurer og vejledninger til rådighed på platforme, hvor der er adgang efter funktionsmæssigt behov.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Alle ændringer til systemer er styret og underlagt den fælles Change management proces. Ændringer og styring heraf dokumenteres i Service Management System, hvori de nødvendige godkendelser ligeledes registreres.	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der foretages risikovurdering og prioritering af den enkelte ændring	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Kunder varsles, forinden ændringsarbejdet, for at sikre mindst mulig gene for kunderne	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret overvågning og registrering af kundernes it-miljøer hos de kunder, der har krav om styring af kapaciteten, for at forhindre systemnedbrud	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect har opdelt it-miljøer i udviklings-, test- og driftsmiljøer for de kunder, der har stillet krav herom	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

Alle relevante enheder i GlobalConnect ' infrastruktur er opdateret med godkendt malware software	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Malware software er opdateret med seneste version (signaturfil).	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Alle kunder med backupaftaler får foretaget backup af data, nogle via underleverandør og andre internt i GlobalConnect	Vi har interviewet relevant personale hos GlobalConnect. Backup foregår til GCOS egne servere. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Kunder med restoreaftaler får foretaget restoretest i henhold til aftalerne	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret registrering og håndtering af alle relevante hændelser	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation. Der er set på registreringer i både service management systemet samt gennemgået hvad der dukker op i de forskellige funktioner på overvågningsskærme og hvorledes incidents håndteres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret overvågning af kunders servere med henblik på tilgængelighed og systemfejl	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation. Der er set på registreringer i både service management systemet samt gennemgået hvad der dukker op i de forskellige funktioner på overvågningsskærme og hvorledes incidents håndteres.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er indført procedurer for, at alle aktiviteter, som er udført af systemadministrator eller med administrative rettigheder, registreres.	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation. Sikkerhedsmodellen fra almindelig bruger til admi-	Vi har ikke ved vores test konstateret væsentlige afvigelser.

	nistrator og domainadministrator brugere er gennemgået og det er påset at der sker registrering og overvågning af aktiviteterne.	
Der er etableret infrastrukturmæssige komponenter som tidsynkroniseres op imod centrale NTP-servere	Vi har interviewet relevant personale hos GlobalConnect. Vi har set dokumentation for at der findes NTP servere og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 13:

Kommunikationssikkerhed

At sikre beskyttelse af informationer i netværk og sikre beskyttelse af understøttelse af informationsbehandlingsfaciliteter.		
GlobalConnect kontroller	Revisors test af kontroller	Resultat af test
Der er etableret formelle forretningsgange for at sikre interne og eksterne overførsler af fortrolige eller følsomme informationer eller data, hvor dette er påkrævet	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret fjernadgang til GlobalConnects systemer for kunder der ønsker dette. Adgangen sker enten gennem offentlige netværk, beskyttet med VPN eller MPLS og firewall	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 14:

Anskaffelse, udvikling og vedligeholdelse af systemer

Det skal sikres, at informationssikkerhed er en integreret del af informationssystemer gennem hele livscyklussen. Dette omfatter også kravene til informationssystemer, som leverer tjenester over offentlige netværk. Sikre at informationssikkerhed tilrettelægges og implementeres inden for informationssystemers udviklingslivscyklus samt sikre beskyttelse af data, som anvendes til test.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Der er etableret formelle processer og procedurer for alle ændringer som foretages i eget it-miljø	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen for Change på netværk og server miljøerne og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret formelle forretningsgange og procedurer for implementering af software i egne og kundens miljøer	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen særligt for projekter og Change og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er implementeret formelle processer og procedurer (Patch Management) for sikkerhedsmæssig opdatering af operativsystemer	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 15:

Leverandørforhold

Eksterne samarbejdspartnere skal overholde virksomhedens fastlagte rammer for it-sikkerhedsniveau.		
GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Alle relevante leverandører har indgået en NDA med GlobalConnect og er i øvrigt bekendt med indholdet af vores sikkerhedshåndbog	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation for retningslinjerne på området.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret forretningsgange som sikrer, at der føres tilsyn med leverandørens etablerede kontroller i form af indhentelse af ISAE 3402 revisorerklæring	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 16:

Styring af informationssikkerhedsbrud

At opnå at sikkerhedshændelser og svagheder i virksomhedens informationsbehandlingssystemer rapporteres på en sådan måde, at det er muligt at foretage korrektioner rettidigt.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Alle sikkerhedsbrud (security incidents) håndteres i Service Management Systemet og i henhold til etablerede procedurer	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
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	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
Der er etableret processer og procedurer, som sikrer, at sikkerhedshændelser registreres og håndteres af rette medarbejdere	Vi har interviewet relevant personale hos GlobalConnect. Vi har gennemgået arbejdsgangen og modtaget dokumentation.	Vi har ikke ved vores test konstateret væsentlige afvigelser.

KONTROLMÅL 17:

Informationssikkerhedsaspekter ved nød-, beredskabs- og reetableringsstyring

Beredskabsstyring skal modvirke afbrydelser i virksomhedens forretningsaktiviteter, beskytte kritiske informationsaktiver mod effekten af et større nedbrud eller en katastrofe samt sikre hurtig reetablering.

GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
Der er udarbejdet en oversigt over beredskabsplaner for relevante funktionsområder som sikrer forretningens videreførelse ved sikkerhedshændelser	Vi har interviewet relevant personale hos GlobalConnect. Vi er blevet oplyst at denne oversigt ikke findes, men at summen består af de respektive funktioners incidentprocedurer, der er stillet til rådighed internt.	Vi har ikke ved vores test konstateret væsentlige afvigelser
GlobalConnect har etableret periodisk afprøvning af beredskabsplaner med formålet at sikre, at beredskabsplanerne er tidssvarende og effektive i kritiske situationer.	Vi har interviewet relevant personale hos GlobalConnect. Der testes 1-2 gange årligt.	Vi har ikke ved vores test konstateret væsentlige afvigelser
Beredskabstests dokumenteres ved rapporter fra øvelserne	Vi har interviewet relevant personale hos GlobalConnect. Der testes 1-2 gange årligt. Vi har fået forelagt dokumentation for test.	Vi har ikke ved vores test konstateret væsentlige afvigelser
Der er etableret redundans i relevante systemer for de kunder, der har krav herom, for at imødekomme tilgængelighedskrav	Vi har interviewet relevant personale hos GlobalConnect. Der er generelt etableret redundans. Vi har modtaget dokumentation for det redundante setup.	Vi har ikke ved vores test konstateret væsentlige afvigelser

KONTROLMÅL 18:

Overensstemmelse med lov og kontraktskrav

Der sikres at informationssikkerhed er implementeret så det overholder organisationens krav og politikker, samt at lov-, myndigheds- eller kontraktskrav ikke overtrædes.		
GlobalConnects kontroller	Revisors test af kontroller	Resultat af test
GlobalConnect har identificeret alle relevante lov- og myndighedskrav	Vi har interviewet relevant personale hos GlobalConnect. GC har identificeret relevante love og myndighedskrav.	Vi har ikke ved vores test konstateret væsentlige afvigelser.
GlobalConnect er ISO9001 og ISO27001 certificeret. Som en del heraf er der udarbejdet procedurer for årlig revurdering og godkendelse af underliggende politikker, proces- og procedurebeskrivelser	Vi har interviewet relevant personale hos GlobalConnect. Kun Global Connect Outsourcing Services er certificeret i begge standarder.	Vi har ikke ved vores test konstateret væsentlige afvigelser.