ISAE 3402 REPORT FOR THE PERIOD 1 JANUARY TO 31 DECEMBER 2016 ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO THE OPERATION OF DARK FIBER, TRANSMISSION AND DATA CENTER SOLUTIONS

GLOBALCONNECT A/S

This document is an unofficial translation of the original Danish text, and in case of any discrepancy between the Danish text and the English translation, the Danish text shall prevail

BDO

CONTENT

AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO THE OPERATION OF DARK FIBER, TRANSMISSION AND DATA CENTER SOLUTIONS

To: The Management of GlobalConnect A/S
GlobalConnect A/S' Customers and their Auditors

Scope
We have been engaged to report on GlobalConnect's (the service organization) description at pages 7-15 of operating services and related controls according to the operations of Dark Fiber, Transmission and Data Center solutions (the description), and on the design and operation of controls related to the control objectives stated in the description.

The Service Organization's Responsibilities
At pages 5-6 of this report, the service organization has prepared an statement on the suitability of the overall presentation of the description and the suitability and operating effectiveness of the designed controls, which are related to the control objectives stated in the description.

The service organization is responsible for: preparing the description and the accompanying statement, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives; identifying the risks threatening achievement of the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Auditor's Independence and Quality Assurance
We have complied with the independence requirements and other ethics requirements in IESBA's rules of ethics which are based on fundamental principles on integrity, objectivity, professional competentes and due care, confidentiality and professional conduct.

We apply ISQC 1 and maintain a comprehensive system for quality assurance, including documented policies and procedures for complying with rules of ethics, professional standards and applicable requirements according to legislation and other regulation.

Service Auditor's Responsibilities
Our responsibility is to express an opinion on the service organization's description and on the design and operation of controls related to the control objectives stated in that description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization and described at pages 5-6.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of Control at a Service Organization

The service organization's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described at pages 5-6 of the service organization's statement. In our opinion, in all material respects:

a. The description presents fairly the systems and related IT general controls in connection with operation of Dark Fiber, Transmission and Data Center solutions as designed and implemented throughout the period from 1 January to 31 December 2016; and

b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January to 31 December 2016; and

c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January to 31 December 2016; and

d. That the controls within Risk Assessment and Treatment, Security Policy, Organization of Information Security, Asset Management, Human Resources Security, Physical and Environmental Security, Communications and Operational Management, Access Controls, Information Security Incident Management, Business Continuity Management and Compliance are in agreement with the requirements of ISO 27001 on Information security management systems and ISO 27002 on Rules governing information security management; and

e. That the organization and design of the controls within the relevant areas were aimed at the requirements in ISO 22301 "Business Continuity Management Systems",

f. That the organization and design of the controls within the relevant areas were aimed at the requirements in Executive Order no. 445 of 11 May 2011 on information security and disaster recovery for electronic communication networks and services, in force until 30 June 2016,

g. That the organization and design of the controls within the relevant areas were aimed at the requirements in "Executive Order no. 462 of 23 May 2016 on the security of personal data in connection with provision of public electronic communication services" and "Executive Order no. 567 of 1 June 2016 on information security and disaster recovery in networks and services", in force from 1 July 2016.

Description of Tests of Controls

The specific controls tested and the results of those tests are listed at pages 17-33.

Intended Users and Purpose
This report is intended only for the customers of the service organization and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Copenhagen, 24 February 2017

BDO Statsautoriseret revisionsaktieselskab

Per Sloth
Partner, Head of Risk Assurance
Registered Public Accountant

Torben Bjerre-Poulsen
Partner
State Authorised Public Accountant

GLOBALCONNECT A/S' STATEMENT

GlobalConnect A/S has prepared the following descriptions of services and relevant controls relating to Dark Fiber, Transmission and Datacenter solutions.
The description is intended for GlobalConnect A/S' customers and their auditors, who have a sufficient understanding to consider it, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements of the customers' financial statements.
GlobalConnect A/S hereby confirms that:

1. The accompanying description fairly presents the services provided by GlobalConnect A/S and the relevant controls relating to Dark Fiber, Transmission and Tele Housing solutions throughout the period from 1 January to 31 December 2016.

We will account for:

- The services provided.
- Relevant control objectives and controls designed to achieve these objectives, including controls to ensure confidentiality, integrity and accessibility of systems and data,
- Relevant control objectives and controls to achieve these objectives, according to the ISO 27001 standard on "Information technology – Security techniques – Information security management systems – Requirements" and ISO 27002 standard on "information security – security techniques – code of practice for information security management".
- Controls to fulfil the requirements of Executive Order no. 445 of 11 May 2011 on information security and disaster recovery for electronic communication networks and services, in force until 30 June 2016.
- Controls to fulfil the requirements of Executive Order no. 462 of 23 May 2016 on the security of personal data in connection with provision of public electronic communication services" and "Executive Order no. 567 of 1 June 2016 on information security and disaster recovery in networks and services", in force from 1 July 2016.
- Other relevant aspects of GlobalConnect A/S' control environment, risk assessment process and information systems of relevance for the operations and used for the treatment and reporting of the services to our customers.

The description includes:

- Relevant information throughout the period from 1 January to 31 December 2016 relating to changes to GlobalConnect A/S' services and accompanying controls, which have been fully documented as incidents, recorded in GlobalConnect A/S' Service Management system.

The description does not include and distort:

- Information relevant to the scope of the described services and accompanying controls, while considering that the description has been prepared to comply with the general requirements of a broad range of customers and their auditors and therefore cannot include every aspect that the individual customers may consider of importance for their specific situation.

2. The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January to 31 December 2016.

The criteria used in making this statement were that:

- The risks that threatened achievement of the control objectives stated in the description were identified;
- The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent achievement of the stated control objectives;
- The controls were consistently applied as designed, including that manual controls were applied by individuals having adequate competences and authority throughout the period from 1 January to 31 December 2016;
- The controls within:
    - Risk Assessment and Treatment
    - Security Policy
    - Organization of information Security
    - Asset Management
    - Human Resources Security
    - Physical and Environmental Security
    - Communications and Operational Management
    - Access Controls
    - Information Security Incident Management
    - Business Continuity Management
    - Compliance

  are in agreement with the requirements of the ISO 27001 standard on "Information technology – Security technics – Information security management systems – Requirements" and the ISO 27002 standard on "Information security – Security technics - Rules governing information security management".
- The organization and design of the controls within the relevant areas were aimed at the requirements in ISO 22301 "Business Continuity Management Systems",
- The organization and design of the controls within the relevant areas were aimed at the requirements in Executive Order no. 445 of 11 May 2011 on information security and disaster recovery for electronic communication networks and services, in force until 30 June 2016,
- The organization and design of the controls within the relevant areas were aimed at the requirements in "Executive Order no. 462 of 23 May 2016 on the security of personal data in connection with provision of public electronic communication services" and "Executive Order no. 567 of 1 June 2016 on information security and disaster recovery in networks and services", in force from 1 July 2016.

Taastrup, 24 February 2017

Christian Holm Christensen
CEO - Chief Executive Officer

GLOBALCONNECT A/S' DESCRIPTION

DESCRIPTION OF SERVICES AND ACCOMPANYING CONTROLS RELATING TO DARK FIBER, TRANSMISSION AND DATA CENTER SOLUTIONS

GENERAL DESCRIPTION OF GLOBALCONNECT A/S

GlobalConnect A/S is provider of Dark Fiber, Transmission and Data Center solutions in Denmark, Northern Germany and parts of Sweden to a number of national and international telecom companies providing services to private and public businesses, universities and educational institutions. Services are also provided to Danish businesses.

GlobalConnect A/S' vision is to be the leading telecom and data communications service provider in Denmark and one of the key players in the markets where we are operating. GlobalConnect A/S will work for: Free fibernet to all as a condition for a developing knowledge society.

General description of the GlobalConnect A/S organization

Internal organization of GlobalConnect A/S:

- A Management consisting of 4 directors who constitute the senior management in the company
- A sales organization with offices in Tåstrup, Stilling, Odense and Hamburg.
- A Systems Design and Sales Support department
- A Marketing department
- A Production department with the subdivisions Fiber Implementation, Transmission Implementation, Logistics department, Project Management and Contract Management.
- An Operations department with OMC, 2nd level operations, Service and Quality Management and Infrastructure development
- A Data Center department with all Global Connect A/S' Data Center operations, maintenance and building activities
- An IT department with Operations and Support, Business Support Systems and Operations Support system
- Executive functions for Finance, HR, Legal and Administration.
- And a number of subsidiaries providing tele-related services, typically based on services purchased from GlobalConnect A/S.

The current description of GlobalConnect A/S' organization is shown below with a chart for the implementation and the service organization.

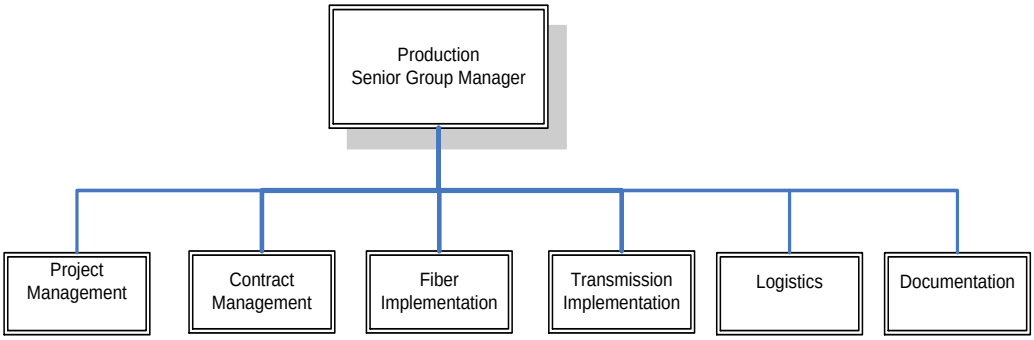
Production

GlobalConnect A/S has for organizational purposes divided the Production department into an implementation department – internally called Production and a service department - divided into an entity for Project Management and an entity for Contract Management. The Logistics function is also a part of the Production department.

Implementation organization

The implementation organization houses the project managers and is responsible for the project until it is put into operation. When the project has been put into operation, the overall responsibility passes to Operations. If errors are reported, technicians from the implementation organization will be called to perform repair.

Approx. 50 people are attached to the implementation organization.



Project Management has the overall responsibility for project coordination and communication during the performance of the projects. All implementation processes are coordinated internally and externally. Project Management will always be informed an upated on the current progress of projects.

Contract Management is responsible for validation of contracts for the purpose of invoicing and debtor handling, making it the most important customer contact in the daily work where it will constitute GlobalConnect A/S' customer service.

Fiber Implementation - Digging work: charting of trace, examination of existing piping and wiring system and treatment by authorities. The next step is specification of requirements, contracting, management of contractors, inspection and handing-over. Project management, time management, economy, suppliers, responsibility for progress and quality of the assignment, including communication with the customer, authorities, suppliers, contractors and end-users, if possible.

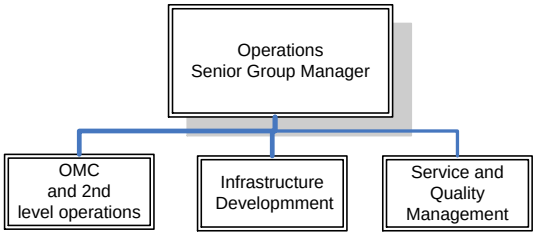
Subcontractors are used for digging and underboring work. Splicing of fibers is primarily performed by GlobalConnect A/S' staff, however, in case of heavy workloads, subcontractors may be used for splicing of new fiber runs and planned changes of the network.

Transmission Implementation – Network element, including specification of requirements, installation of active equipment, quality and testing requirements, tenders and handing-over. Project management, time management, economy, suppliers, responsibility for progress and quality of the assignment, including communication with the customer, authorities, suppliers, contractors and end-users, if possible.

Documentation – documentation of all fibers with accompanying connections in the GIS programs MapInfo and ConnectMaster used in GlobalConnect A/S.

Logistics – responsible for purchases for the project implementation with special focus on GlobalConnect A/S' strategically important suppliers.

All departments have solely GlobalConnect A/S in-house staff. The employees are competent and experienced within their specific workareas as most of them have many years' experience working within telecommunications.



Operations

Approx. 30 people are attached to Operations.

Operations – Day-to-day operations and monitoring of fiber and transmission network, and data sites and amplifier sites. Development and maintenance of GlobalConnect A/S' transmission infrastructure. Quality management, Service management in relation to customers and handling of planned work throughout the organization.

OMC - Operations center, attended 24 hours a day, which monitors, operates and maintains all platforms. In addition, Single Point of Contact for all operating projects. Technicians from "Transmission" perform error recovery for Operations & Maintenance, which is responsible for the operations.

Infrastructure Development - Responsible for expansion and maintenance of GlobalConnect A/S' back-bone network.

Service and Quality Management – Handles identification and description of quality parameters, preparation and maintenance of ISO 9001:2008 quality system, implementation of quality parameters within the organization, including performance and evaluation of internal audit. Quality Assurance is also responsible for disaster recovery testing, Risk Management tasks, statutory requirements in relation to information security and contingency plans for electronic communications networks and services, and Social Responsibility.

In addition, Service and Quality Management performs current service level handling in relation to customers, test and acceptance of solutions delivered to the customers, and general planning and handling of change management.

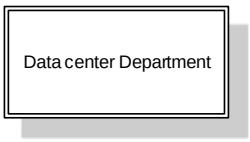
Description of the service organization

In the daytime, 3 - 4 operators in the OMC service customers on first level support, staff with responsibility for planned work in connection with, for example, fiber restructuring, and a technical specialist to handle new operating solutions. Outside normal work hours, there is as a minimum one operator in the OMC.

Second level support has 5 employees at disposal through our technical organization. Third level support has 7 employees at disposal through our infrastructure entity.

Third level support has signed nationwide backup agreements for fiber breaks and two similar nationwide agreements for electricity work. GlobalConnect A/S has always spare parts at its disposal to ensure a quick replacement of defective equipment.

As regards fiber work, digging contractors are used to dig tracé, pipe fitting and insertion of fibers. For new fiber runs, contractors are used to splice the fibers, while primarily own resources are used for error recovery on existing fiber systems.



Data Center

Approx. 10 people are attached to the Data Center department.

Data Center – Handles establishment and operation of Data Center solutions, including allocation of rack-space, power supply, cooling, and alarms.

General description of infrastructure

GlobalConnect A/S provides Dark Fiber solutions, Transmission solutions, and Data Center solutions covering Denmark, Northern Germany and parts of Sweden with a network of optical fibers and several types and sizes of datacenters.

GlobalConnect A/S' provides infrastructure solutions to a large number of tele companies, service organizations and other enterprises and complies for this purpose with the regulatory requirements of the following executive orders: *No. 445 of 11 May 2011 on information security and disaster recovery for electronic communication networks and services, which was in force until 30 June 2016, and "No. 462 of 23 May 2016 on the security of personal data in connection with provision of public electronic communication services" and "No. 567 of 1 June 2016 on information security and disaster recovery in networks and services", which is in force from 1 July 2016.*

GlobalConnect A/S maintains contingency plans for IT, OMC and Data Center solutions and a risk management process, which is updated regularly.

General description of Dark Fiber solutions

GlobalConnect A/S offers sale or lease of "Dark Fiber solutions". The customer leases or purchases a fiber run and receives a confirmation when put into operation from GlobalConnect A/S that the fibers comply with the specified requirements.

GlobalConnect A/S attends Dark Fiber solutions 24 hours a day and error incidents are discovered quickly and error recovery is made without undue delay.

GlobalConnect A/S carries out preventive maintenance by means of route checking, monitoring of sites where other contractors are carrying out digging work, attenuation measurements and correct responding to all relevant pipe inquiries to prevent snipping.

General description of Transmission solutions

GlobalConnect A/S offers Transmission solutions based on Dark Fiber solutions with active transmission equipment placed with the customer. When providing such solutions, GlobalConnect A/S guarantees that they meet the specified service requirements and other technical and specific requirements, including an uptime guarantee.

GlobalConnect A/S monitors all Transmission solutions 24 hours a day to be able to deal promptly with any errors found in the relevant transmission equipment.

GlobalConnect A/S will at any time have spare equipment to replace defective equipment promptly. Improvements and preventive activities are also carried out regularly in the Transmission solutions to secure the best possible uptime.

General description of Data Center solutions in Denmark and Northern Germany

Data Center solutions are today a strategically important element of GlobalConnect A/S' provision of tele services, because datacenters and fiber net interact to provide the customers with the most effective operating conditions for IT services.

The Data Center solutions include a server room in which it is possible to place own racks in a suitable operating environment for servers and other IT and telecom equipment. The customers have access to the facilities 24x7x365.

The Data Center solutions are placed at the node of GlobalConnect A/S' network spine of fiber rings, which forms a big figure "eight" across Denmark, Sweden and Northern Germany. The network's inherent redundancy ensures high transmission security and uptime for our customers' IT services.

GlobalConnect A/S has data centers in both Denmark, Germany and Sweden:

- 20 sites in Taastrup
- 6 sites in Hamburg
- 3 sites in Kolding
- 3 sites in Århus
- 1 site in Albertslund
- 1 site in Central Copenhagen
- 1 site in Odense
- 65 sites in Denmark, Sweden and Northern Germany.

GENERAL CONTROL ENVIRONMENT

GlobalConnect A/S' maintenance of risk and exposure assessment

GlobalConnect A/S performs regularly activities for the purpose of:

1. Analyzing and classifying GlobalConnect A/S' overall infrastructure (operating systems, transmission and cable paths, buildings etc.),
2. Identifying the threats that present the most significant risks,
3. Identifying, selecting and prioritizing the contingency plans in relation to those risks, and
4. Performing an assessment of the importance of the individual infrastructure elements for maintenance of the services internationally, nationally and locally.

The consequences of the risk assessment for the presently most significant 15 threats are differentiated into 4 levels:

1. Total breakdown – none of our services can be provided.
2. Partial breakdown – considerable elements of our network are affected by the breakdown.
3. Local interruption – meaning that only minor local elements of our network will be affected by a breakdown.
4. Incident without interruption of operations – meaning that the relevant incident does not affect our network and services.

Those threats are also assessed in relation to how frequently they are expected to occur according to this scale:

1. Low, 5 years.
2. Medium, 1 year.
3. High degree of probability, several times a year.
4. Very frequent, monthly.

The same, at present most significant 15 threats have been reviewed critically including an exposure assessment in which the preventive measures, which have already been made to deal with the threats, have been considered. Preventive and enhancing measures are performed currently to limit the mentioned threats.

Moreover GlobalConnect A/S performs an annual audit of the risk assessment to ensure that the prioritized risks continue to be the right priorities and to audit the assessment of threat and vulnerability. This ensures that GlobalConnect A/S also complies with the regulatory requirements in the area, see the requirements in the executive orders: *"No. 445 of 11 May 2011 on information security and disaster recovery for electronic communication networks and services, which was in force until 30 June 2016, and "No. 462 of 23 May 2016 on the security of personal data in connection with provision of public electronic communication services" and "No. 567 of 1 June 2016 on information security and disaster recovery in networks and services", which is in force from 1 July 2016.*

GlobalConnect A/S' maintenance and testing of current contingency plans for IT and OMC and Data Center solutions

GlobalConnect A/S has and maintains contingency plans for IT, OMC and Data Center solutions. The plans define the responsibility for maintaining optimal operating reliability, including response time for different levels of critical errors, the process for escalation, the process for dealing with emergencies and communication with customers and media in such situations.

The plans describe the general specifications for the equipment installed for power supply, emergency generators, UPS, cooling, fire extinction, alarm system and access control and the activities performed to maintain those systems for the purpose of current prevention and improvements.

There is an approved plan for testing of both plans. The tests are documented in the Service Management system.

The contingency plans are updated at least every second year and may be distributed to customers at request.

GlobalConnect A/S' monitoring of Dark Fiber solutions and Transmission solutions and the infrastructure of Data Center solutions from an operating center with staff on call 24 hours a day

GlobalConnect A/S' OMC – Operations & Maintenance Center – in Taastrup monitors closely the Dark Fiber solutions, Transmission solutions and Data Center solutions including repeater sites, among others also by video monitoring of entrances and gates to the area. The OMC is staffed 24x7x365.

High security is achieved among others by personal access control, 24/7/365 staff monitoring from OMC inclusive of, among others, video monitoring and advanced fire and intrusion alarms. Any incident or alarm, from access control to fluctuations in the air temperature, is investigated immediately. The power supply is secured by redundant UPS or diesel powered-generators, and the cooling systems are also redundant. All incidents are recorded in a Service Management system.

High physical security is given high priority. Gates, fences, and intrusion alarms and monitoring are important elements when the installations are to be secured against trespassing. All accesses are logged in the ADK system.

The Transmission solutions are designed with a high degree of security, among others by securing redundancy in the design of the networks in the ring structures to ensure that the communication direction may be reversed in case of cable break or failing transmission equipment.

The Data Center solutions are designed with an N+1 redundancy on all critical systems, among others with redundant diesel generators as back-up power.

All centers are monitored from OMC, 24x7x365 and any incident or alarm, from access control to fluctuations in air temperature, are investigated immediately. Power supply is secured by redundant UPS and diesel-powered generators and the cooling systems are also redundant. All incidents are recorded in a Service Management system.

GlobalConnect A/S' control environment and its management

GlobalConnect A/S' quality system is designed to fulfil the requirements of the ISO 9001 standard on quaity requirements. The relevant control environment for current enhancements and preventive measures is the responsibility of the quality organization under the leadership of a quality manager. Meetings are held in GlobalConnect A/S' Quality and IT Security Committee (Kvalitets- og IT-sikkerhed-sudvalg (KSU)), which includes key staff from several different areas in the organization. The purpose of the committee is to discuss issues, at a tactical level, within quality and/or IT security. Issues which are to be escalated in relation to implementation are discussed in GlobalConnect A/S' Quality and IT security Forum (Kvalitets- og IT-sikkerhedsforum (KSF)). This forum includes 4 Executives and Senior Group Managers from Operations and GC-Outsourcing Services and the Quality Managers from these two entities. At these meetings, the Management sets out guidelines and goals for the further quality work in GlobalConnect A/S.

The audit plan for review of all business processes in updated annually at the year-end and it must be approved by KSF.

There is an approved 5-year plan for testing of the contingency plans for IT and Data Center solutions. Both the testing plan and the contingency plans are audited at least every 2nd year as required by the authority within the areas in the Ministry of Defence's entity for handling of information security. The tests carried out according to the plan are documented in our Service Management System based on ITIL (IT Infrastructure Library) and in an electronic folder kept by the Quality Manager, who is responsible for carrying out the tests.

Changes to services and relevant controls

GlobalConnect A/S uses a Service Management system for recording and follow-up and documentation of all incidents in both internal IT systems and customer solutions within Dark Fiber, Transmissions and Data Center solutions. This has enhanced the security considerably when handling errors and breakdown, which are reported by the customers or which are found in connection with the 24-hour monitoring.

The services provided by GlobalConnect A/S and the relevant controls have not been subject to any material changes in the period from 1 January to 31 December 2016.

CONTROL OBJECTIVES AND CONTROLS FOR DARK FIBER SOLUTIONS, TRANSMISSION SOLUTIONS AND DATA CENTER SOLUTIONS ETC.

Dark Fiber solutions

GlobalConnect A/S' major fiber runs are monitored constantly by a fiber test system, which carries out the so-called OTDR measurements on a dedicated fiber. The equipment is monitored 24 hours a day and in case of cable breaks, it is possible to identify, by approx. 1 m accuracy, where the break is. This leads to a short error recovery time in case of snipping.

All incidents are recorded in the Service Management system there the entire course of incidents is documented and may be retrieved.

For a detailed description of the control objectives and controls for Dark Fiber solutions, we refer to Dark Fiber solutions in the schedule.

Transmission solutions

The transmission equipment is monitored 24 hours a day and in case of breakdown, OMC receives an alarm with information on the equipment that is failing.

GlobalConnect A/S opens an error report in the Service Management system on all errors with a reference number which is to be used throughout the subsequent error handling process. The customer is advised

without undue delay based on a pro-active approach to errors which affect the customer's feeling of service. Those tickets will be dealt with immediately so that the traffic is affected as little as possible. During the repair, GlobalConnect A/S will inform the customer regularly of the progress made.

For a detailed description of the control objectives and controls for Transmission solutions, we refer to Transmission in the schedule.

Data Center solutions

To prevent incidents and reduce the risk of break-down, the following inspections are made of all Data Center solutions:

- Quarterly inspection of generators, temperature, fire extinction equipment, UPS systems, battery backup, alarm systems and cleaning condition.
- Annual inspection by external provider of cooling system and load test of generators.
- In case of actual break-down, the customer must be informed, as far as possible, within 10 minutes.
- Statistics are prepared monthly of alarms received and error messages.

According to the quality assurance process for access control, security and alarms, personal access cards and a code are required to obtain access to the facilities. To ensure that the database with information in the control system is fully updated, a quarterly check is made of the access cards that have been used in the most recent period. There is follow-up in relation to customers and suppliers and internally in relation to our HR department.

For a detailed description of the control objectives and controls for Data Center solutions, we refer to Data Center solutions in the schedule.

Operation and monitoring

In our Service Management system, based on ITIL (IT Infrastructure Library), all alarms are recorded from Dark Fiber, Transmission and Data Center solutions. The system documents escalation and activities from receipt of an alarm to error recovery and normal operations. The aim is that error recovery must be started within 30 minutes.

For a detailed description of the control objectives and controls for operation and monitoring, we refer to Dark Fiber solutions, Transmission solutions, Data Center solutions in the schedule.

Planned work

All planned work on all solutions is recorded in the Service Management system in its own category, and OMC is responsible for sending warnings to customers. The warnings are also recorded in the Service Management system. Requests from customers to OMC for this purpose are treated and answered directly and the documentation for the correspondence with the customers is recorded in the Service Management system. After completion and check of the operating status has been restored, the work is reported as completed to the Service Management system and the case is closed.

For a detailed description of the control objectives and controls for planned work, we refer to Dark Fiber solutions, Transmission solutions, Data Center solutions in the schedule.

Internal processes

GlobalConnect A/S has prepared and maintains a quality management system according to the ISO 9001 standard "Quality Management Systems Requirements. The quality management system sets out processes for logic access to our internal IT systems. GlobalConnect A/S' IT department is responsible for logging all logins to the systems.

GlobalConnect A/S' IT department is also resonsible for maintaining the internal procedures to secure segregation of duties when using the internal IT systems.

The backup of GlobalConnect A/S' internal IT operating systems is performed by an external business partner according to a contract. The external partner is obliged to comply with the current ISAE 3402 reporting standard.

For a detailed description of the control objectives and controls for internal processes, we refer to Internal Processes in the schedule.

ISO 27001/27002 Compliance

GlobalConnect A/S ensures compliance with ISO 27001 and 27002 by maintaining and handling the IT security policy, contingency plans, an ISO 9001 quality assurance system and annual updates of a GAP analysis against all relevant requirements of those standards. All systems are subject to regular internal audit which is documented in audit reports. There is follow-up on all deviations found, and efforts are made currently to improve the related processes.

For a detailed description of the control objectives and controls for ISO 27001/27002 Compliance, we refer to ISO 27001/27002 Compliance in the schedule.

ISO 22301 Compliance

Global Connect A/S maintains an IT contingency plan and a Housing and OMC contingency plan to maintain reliable operation in all situations of the IT systems used and a contingency resources which can assist 24 hours a day in connection with operating problems. The contingency plan is tested in accordance with an approved test plan. The results of the tests are documented in the Service Management system.

Global Connect A/S updates annually its Risk Management plan and records all incidents which may present a risk in the daily operation of the solutions. In addition, the requirements of ISO 22301 on management systems – continuation of operations in the internal quality assurance audits.

For a detailed description of the control objectives and controls for ISO 22301 Compliance, we refer to ISO 22301 Compliance in the schedule.

CONTROL OBJECTIVES, CONTROLS, TESTS AND RESULTS OF TESTS

In the following, the relevant control objectives and implemented control activities designed to achieve the control objectives are described and selected by GlobalConnect A/S.

We have described the tests performed that were considered necessary to obtain reasonable assurance that the described control objectives were achieved, and that the relevant controls operated effectively in the period from 1 January to 31 December 2016.

The tests of the design, implementation and operating effectiveness of controls were performed by inquiries, inspection, observation, and re-performance.

Type	Discription
Inquiry	Inquiries of relevant personnel at GlobalConnect A/S have been performed for all significant control activities. The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, and whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorizations and access controls, data transmission and inspection of equipment and locations.
Observation	The use and existence of specific controls has been observed, including tests to ensure that the control operated effectively.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Frontsafe A/S within back-up of the operating systems, we have from the independent auditor received a report on the IT general controls related to the operation of Frontsafe Cloud Backup services in the period from 1 May 2015 to 30 April 2016. This service sub-organization's relevant control objectives and related controls are not included in GlobalConnect A/S' description of services and relevant controls related to operation of Dark Fiber, Transmission and Data Center solutions. Accordingly, we have solely assessed the report and tested the controls at GlobalConnect A/S that monitor the functionality of the service sub-organization's controls.

General control environment		
Control objectives • *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*		
Control activity	**Test performed by BDO**	**Result of test**
Infrastructure • GlobalConnect A/S' infrastructure of cables, transmission equipment and buildings is registered and documented.	We have made inquiries of relevant staff and inspected procedures for recording of information on the infrastructure. We have observed the systems used for recording of the specific areas in the infrastructure.	No deviations were found.
Threats • GlobalConnect A/S identifies and records the threats that present the most significant risks.	We have made inquiries of relevant staff and inspected the risk and exposure assessment, procedures and policies. We have observed that the review of the individual areas is operated in the Service Management system to ensure a current assessment of risks and maintenance of procedures and controls.	No deviations were found.
Contingency plans • GlobalConnect A/S prioritizes contingency plans in relation to the risks. • Global Connect A/S assesses the importance of the specific infrastructure elements for maintenance of the services internationally, nationally and locally. • Global Connect A/S maintains contingency plans. • Global Connect A/S tests contingency plans.	We have made inquiries of relevant staff and inspected the service organization's 'Contingency Plan for IT" and Contingency Plan, OMC and Housing. We have compared these with the service organization's risk and vulnerability assessments and processes and policies. We have inspected that plans are available for testing and maintenance of the contingency plans which ensure a current assessment of the individual infrastructure elements. We have inspected the plan and follow-up plan for contingency tests and documentation of contingency tests performed.	No deviations were found.

Dark Fiber solutions		
Control objectives • *To ensure correct and safe operation of information processing equipment.* • *To detect unauthorized information processing activities.* • *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*		
Control activity	**Test performed by BDO**	**Result of test**
Monitoring • OMC monitors Dark Fiber solutions currently. • All alarms and incidents are documented in the Service Management system. • All alarms that cannot be closed immediately by OMC are escalated to 2nd level support for remedy.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed that the monitoring is dealt with by the OMC in Taastrup 24/7/365, and that the OMC is staffed at 2nd level support. We have observed that alarms and incidents are documented in the Service Management system. We have selected cases by random sampling from the Service Management system and inspected the relevant documentation.	No deviations were found.
Repair • All errors found are documented in the Service Management system. • All repairs of Dark Fiber is documented in the Service Management system. • Planned changes of cable runs comply with accepted quality process by: - Determination of time frame for the change. - Warning of affected customers - Change of cabling - Go-ahead to customers - The progress of all planned changes is documented in the Service Management system.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed that repairs of Dark Fiber are completed by a go-ahead to the customer and may be completed by splice measurements if desired by the customer. We have observed that the affected customers are warned in connection with planned changes and that go-ahead is awaited from the customers before the change is started. We have observed that the planned changes are documented in the Service Management system.	No deviations were found.
Risk analysis • GlobalConnect A/S' risk plan includes the 15 top priority risks of which 2 concern Dark Fiber solutions. • The risk plan is audited at least once a year.	We have made inquiries of relevant staff and inspected the service organization's risk and exposure assessment. We have observed that the risk and exposure assessment includes a risk plan with the 15 top priority risks, of which 2 concern Dark Fiber solutions. We have observed that the risk assessment and vulnerability analysis are updated annually.	No deviations were found.

Dark Fiber solutions		
Control objectives • *To ensure correct and safe operation of information processing equipment.* • *To detect unauthorized information processing activities.* • *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*		
Control activity	**Test performed by BDO**	**Result of test**
Contingency plan • GlobalConnect A/S' contingency plan for Dark Fiber solutions is tested regularly in accordance with an approved plan for testing of contingency plans. • The contingency plans are updated at least every second year. • The result of the tests is documented in the Service Management system and in a manual file.	We have made inquiries of relevant staff and inspected the service organization's 'Contingency Plan, OMC and Housing. We have compared these with the service organization's risk and vulnerability assessments and processes and policies. We have observed that incidents relating to Dark Fiber are recorded in the OMC. The incidents that cannot be immediately dealt with by the OMC 1st level supporters are escalated to the 2nd level support. We have made inquiries of relevant staff and inspected the plan and follow-up plan for contingency testing and documentation for contingency tests performed. We have observed that the contingency plans are updated at least every second year and that the latest version is updated in November 2016. We have observed that tests of the contingency plan are stored both in the Service Management system and manually.	No deviations were found.
Data communication • Delivered Dark Fiber solutions are measured to ensure that the connection complies with the relevant standards (ITU-T Recommendation G.652 and G.655) and specifications for Dark Fiber. • The measurements are documented by certificates and relevant measurement reports. • Dark Fiber solutions are terminated at the customer. • The responsible project manager performs inspection at the address of delivery and building. • The termination room is inspected to ensure that that the delivery is exactly as ordered. • The results of the inspections are documented by the responsible project manager.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed that delivered Dark Fiber solutions are measured to ensure that the connection complies with the relevant standards and specifications for dark fiber. We have inspected selected certificates and selected reports of the measurements performed. We have observed that the measurements are documented by certificates and relevant measurement reports.	No deviations were found.

Dark Fiber solutions		
Control objectives • *To ensure correct and safe operation of information processing equipment.* • *To detect unauthorized information processing activities.* • *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*		
Control activity	**Test performed by BDO**	**Result of test**
Dark Fiber solutions to customers are protected against loss of authenticity, integrity, traceability, accessibility and confidentiality by always ensuring physical separation from all other networks.	We have observed that there is always minimum one project manager who is responsible for inspection of the address of delivery, the building and termination room. We have observed that the inspections are documented and relate to the specific project. We have inspected selected reports of inspections performed. We have observed that installations attached to fiber installations are documented in the CircuitID database by a unique number, comprising a code for the installation containing codes for: • Capacity (boxes) • Fiber connections • Racks • Power • Internal cablings • Internal run numbers	

Transmission solutions

Control objectives

- *To ensure correct and safe operation of information processing equipment.*
- *To detect unauthorized information processing activities.*
- *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*

Control activity	Test performed by BDO	Result of test
Monitoring and error handling • OMC monitors the cables used, housing facilities, equipment nodes and circuits by means of remote monitoring, which among others monitors configuration, error handling, transmission quality and security handling. • All recorded incidents are documented in the Service Management system. • All error handling of Transmission solutions supplied GlobalConnect A/S is performed by OMC. • All incidents are documented in the Service Management system where the entire course from alarm or other identification to final error recovery is recorded, including 2nd level support and additional support.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed the monitoring in the service organization's OMC. We have observed that incidents are recorded in the Service Management system. We have observed that error handling of transmission solutions, provided by GlobalConnect A/S, is dealt with by the OMC. We have selected cases by random sampling from the Service Management system and inspected the relevant documentation and observed that the entire course is recorded, including escalation to 2nd level support and additional escalation.	No deviations were found.
Network administration • OMC performs network administration for both planned work and critical maintenance in close cooperation with the customer's contact person. • This work is performed in accordance with approved and described processes and is documented in the Service Management system.	We have made inquiries of relevant staff at the service organizations, inspected procedures and guidelines for business processes in OMC and observed business processes in the service organization's OMC. We have observed that both planned work and critical maintenance are performed in cooperation with the customer, and documented in the Service Management system. We have inspected selected documentation for the network administration for both planned work and critical maintenance.	No deviations were found.

Transmission solutions

Control objectives

- *To ensure correct and safe operation of information processing equipment.*
- *To detect unauthorized information processing activities.*
- *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*

Control activity	Test performed by BDO	Result of test
Planned work • Planned changes of cable runs follow an approved quality process where a time frame is fixed for the change, warning of affected customers, change of cabling and go-ahead to the customer. The progress of all planned changes is documented in the Service Management system.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed that the affected customers are warning in connection with planned changes, and that a go-ahead is awaited from the customers before the change is started. We have observed by random sampling that planned changes are documented in Service Management.	No deviations were found.
Contingency Plan • GlobalConnect A/S' contingency plan for Transmission solutions is tested regularly in accordance with an approved plan for testing of contingency plans. • The contingency plans are updated at least every second year. The result of the tests is documented in the Service Management system and in a manual file.	We have made inquiries of relevant staff and inspected the service organization's 'Contingency Plan, OMC and Housing. We have compared these with the service organization's risk and vulnerability assessments and processes and policies. We have observed that incidents relating to Transmission equipment are recorded in the OMC. The incidents that cannot be immediately dealt with by the OMC 1st level supporters are escalated to the 2nd level support. We have made inquiries of relevant staff and inspected the plan and follow-up plan for contingency testing and documentation for contingency tests performed. We have observed that the contingency plans are updated at least every second year and that the latest version is updated in November 2016. We have observed that tests of the contingency plan are stored both in the Service Management system and manually.	No deviations were found.

Data Center solutions

Control objectives

- *To ensure correct and safe operation of information processing equipment.*
- *To detect unauthorized information processing activities.*
- *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*
- *To prevent unauthorized physical access to, damage of and interruption of the enterprise's premises and information.*
- *To avoid loss, damage, theft or compromising of assets and interruption of business activities.*

Control activity	Test performed by BDO	Result of test
Monitoring • GlobalConnect A/S' OMC monitors all Data Center solutions in operation by means of remote monitoring which, among others, monitors alarms relating to temperature, fire, water, access etc. • All recorded incidents are documented in the Service Management system, where escalation and error handling are also documented.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed the monitoring in the service organization's OMC. We have selected cases by random sampling from the Service Management system and inspected the relevant documentation and observed that the recorded incidents are documented.	No deviations were found.
Access control • All facilities of Data Center solutions have an access control system to ensure that only authorized and approved employees and customer appointed persons have access to these facilities. • All activities are recorded in the OMC's ADK register. • Approval, issue and closing of access media and the current maintenance of the area follow GlobalConnect A/S' quality process.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have observed the setup of the access control system and inspected the documentation for creation of access cards and rights granted. We have inspected extracts form the ADK register for selected Data Centers and repeater stations (sites). We have observed the monitoring of the access control in the service organization's OMC. We have selected by random sampling and inspected documentation for creations and closings in accordance with the service organization's quality process in this respect.	The half-yearly control of all open employee access cards, which have not been used for six months, has not been performed as expected. Request forms for temporary access cards were in several cases not completed with sufficient information or were attached as documentation in the Service Management system.

Data Center solutions

Control objectives

- *To ensure correct and safe operation of information processing equipment.*
- *To detect unauthorized information processing activities.*
- *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.*
- *To prevent unauthorized physical access to, damage of and interruption of the enterprise's premises and information.*
- *To avoid loss, damage, theft or compromising of assets and interruption of business activities.*

Control activity	Test performed by BDO	Result of test
Preventive maintenance • GlobalConnect A/S performs, quarterly, preventive inspections of all Data Center facilities and quarterly inspection of sites in accordance with the process described in the quality management system for Housing operations. • The result of the inspections is documented in completed schedules. • Subsequent performance of maintenance work is documented in the Service Management system.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have inspected the documentation for the quarterly inspections for selected telecommunication buildings and repeater stations (sites).	No deviations were found.
Physical security • Global Connect A/S complies with specified requirements for the physical security of the Data Center solutions, comprising: - Building - Floors - Footprints - Climate - Electricity - Access - Alarm monitoring - Fire - Cabling	We have made inquiries of relevant staff and inspected descriptions and external agreements for maintenance. We have observed the physical conditions for selected telecommunication buildings and repeater stations (sites) and verified that these are based on individual risk assessments.	No deviations were found.
Physical security - Data Center 1, Wedenstrasse Hamburg • Global Connect A/S complies with specified requirements for the physical security of the Data Center solutions, comprising: - Building - Floors - Footprints - Climate - Electricity - Access	We have made inquiries of relevant staff and inspected descriptions and external agreements for maintenance. We have observed the physical conditions for the Data Center. We have observed that the data center has manual fire extinction.	No deviations were found.

Data Center solutions		
Control objectives • *To ensure correct and safe operation of information processing equipment.* • *To detect unauthorized information processing activities.* • *To prevent interruption of business activities and protect critical business processes against the impact of major crashes of information systems or disasters, and to ensure a timely restore.* • *To prevent unauthorized physical access to, damage of and interruption of the enterprise's premises and information.* • *To avoid loss, damage, theft or compromising of assets and interruption of business activities.*		
Control activity	**Test performed by BDO**	**Result of test**
- Alarm monitoring - Fire - Cabling		
Contingency plan • GlobalConnect A/S' contingency plan for Data Center solutions is tested regularly in accordance with an approved plan for testing of contingency plans. • The contingency plans are updated at least every second year. • The result of the tests is documented in the Service Management system and in a manual file.	We have made inquiries of relevant staff and inspected the service organization's 'Contingency Plan for IT" and Contingency Plan, OMC and Housing. We have compared these with the service organization's risk and vulnerability assessments and processes and policies. We have observed that incidents relating to Data Center are recorded in the OMC. The incidents that cannot be immediately dealt with by the OMC 1st level supporters are escalated to the 2nd level support. We have made inquiries of relevant staff and inspected the plan and follow-up plan for contingency testing and documentation for contingency tests performed. We have observed that the contingency plans are updated at least every second year and that the latest version is updated in November 2016. We have observed that tests of the contingency plan are stored both in the Service Management system and manually.	No deviations were found.

Internal processes

Control objectives

- *To control the access to information.*
- *To ensure unauthorized user access and prevent unauthorized access to information systems.*
- *To prevent unauthorized user access and compromising or theft of information and information processing equipment.*
- *To prevent unauthorized access to network services.*
- *To prevent unauthorized access to operating systems.*
- *To implement and maintain an adequate level of information security and services in accordance with agreements for service from third parties.*
- *To maintain integrity and availability of information and information processing equipment.*

Control activity	Test performed by BDO	Result of test
Logical access • GlobalConnect A/S complies with the processes of the quality management system for administration of logical access to internal IT systems. • The HR department is responsible for monitoring the employees' access to the IT systems. GlobalConnect A/S' IT department is responsible for logging, monitoring and administration of all logical access to internal IT systems.	We have made inquiries of relevant staff and inspected descriptions of procedures. We have selected by random sampling and inspected documentation for operations, including: • Creation and closing documents. • Documentation for review of created users and relevant rights.	No deviations were found.
Segregation of duties • GlobalConnect A/S maintains internal procedures to ensure segregation of duties in and around technical IT systems. • GlobalConnect A/S uses the logical access control function to support the segregation of duties.	We have made inquiries of relevant staff at the service organization. We have inspected that segregation of duties is ensured by having user groups with different rights in the service organization's IT systems. We have observed that segregation of duties, by granting rights to user groups in the service organization's IT systems, is a part of the process relating to logic access control.	No deviations were found.
Back-up • GlobalConnect A/S uses a 3rd party organization (Frontsafe) for backup of the operating programs. • Frontsafe has documented its controls in a current ISAE 3402 assurance report.	We have made inquiries of relevant staff at the service organization. We have observed that the service organization uses Frontsafe A/S for external back-up, and that Frontsafe A/S has an ISAE 3402 assurance report for the period from 1 May 2015 to 30 April 2016. We have observed that the service organization documents the back-up process including the scope of the back-up.	No deviations were found.

ISO 27001/27002 Compliance		
Control objectives: Risk Assessment and Treatment • *To reduce risks caused by exploitation of known technical weaknesses.* • *To ensure that information security incidents and weaknesses relating to information systems are communicated in such a manner that corrective action may start in time.*		
Control activity	**Test performed by BDO**	**Result of test**
Risk Assessment and Treatment • GlobalConnect A/S updates its Risk Management plan annually. • GlobalConnect A/S records all incidents which may present a risk in relation to the daily operation of the solutions in the Service Management system.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - General control environment - Infrastructure. - Dark Fiber solutions - Monitoring, Risk analysis. - Transmission solutions – Monitoring and error handling. - Data Center solutions – Monitoring.	No deviations were found.
Control objectives: Security Policy • *That management shows the direction of and supports information security in accordance with business requirements and relevant legislation and regulations.* • *To ensure that systems comply with the requirements of the company's security policies and security standards.*		
Control activity	**Test performed by BDO**	**Result of test**
Security Policy • GlobalConnect A/S has at any time an approved IT security policy. • The approved IT security policy has been communicated effectively to all employees. • The approved IT security policy is included in the policy for information security approved by management. • The organisation contributes to the annual updating of the IT security policy. • The responsibility for the policy has been placed and accepted by the employees.	We have made inquiries of relevant staff at the service organization. We have inspected documentation that the IT security policy is updated and approved annually by the service organization's management. We have observed that the staff at the service organization is familiar with the IT security policy and that it is accepted annually.	No deviations were found.

ISO 27001/27002 Compliance

Control objectives: Organization of Information Security

- *To control information security in the company.*
- *To maintain the security of the company's information and information processing equipment to which external parties have access, or which is processed, communicated to or dealt with by external parties.*
- *To avoid breach of legislation, statutory, regulatory or contractual liabilities and security requirements.*
- *To ensure a uniform and effective method for control of breach of information security.*

Control activity	Test performed by BDO	Result of test
Organization of information Security • Employees and external partners are instructed to not pass on classified information to any third parties which is also a regulatory requirement in Executive Order No. 445 of 11 May 2011 on information security and disaster recovery for electronic communication networks and services, which was in force until 30 June 2016, and Executive Order no. 462 of 23 May 2016 on the security of personal data in connection with provision of public electronic communication services, which is in force from 1 July 2016 and which GlobalConnect A/S must comply with.	We have made inquiries of relevant staff at the service organization. As regards the employees of the service organization, we refer to ISO 27001/27002 Compliance - Security Policy. We have inspected the partner agreement signed by the service organization and Frontsafe A/S.	No deviations were found.

Control objectives: Asset Management

- *To obtain and maintain adequate protection of the company's assets.*
- *To maintain integrity and availability of information and information processing equipment.*
- *To ensure protection of information in networks and protection of the underlying infrastructure.*
- *To ensure an adequate protection level for information.*

Control activity	Test performed by BDO	Result of test
Asset Management • The responsibility for identification and documentation of all GlobalConnect A/S' IT assets has been defined. • Rules have been set up for classification of GlobalConnect A/S' IT information.	We have made inquiries of relevant staff at the service organization. We have observed that the service organization's IT assets have been identified and documented. We have observed that a classification has been performed based on formally determined rules for classification.	No deviations were found.

ISO 27001/27002 Compliance

Control objectives: Human Resources Security

- *To assure that employees, contractors and external users understand their responsibilities and are qualified for the tasks they will be performing, and to reduce the risk of theft, fraud or misuse of facilities.*
- *To assure that all employees, contractors and external users are aware of security threats and security issues, their responsibilities and duties and are able to support the company's security policy when performing their common work, and reduce the risk of human errors.*
- *To assure that termination or change of the employment of employees, contractors and external users takes place in a proper manner.*

Control activity	Test performed by BDO	Result of test
Human Resources Security • Rules have been defined for GlobalConnect A/S' employees with respect to responsibilities, background check and an approved standard employment contract. • GlobalConnect A/S has an approved process for education and training of employees. • GlobalConnect A/S has an approved process to ensure that the properties of GlobalConnect A/S are returned and that all IT accesses are removed on resignation.	We have made inquiries of relevant staff at the service organization. We have inspected selected employment contracts and criminal records. We have inspected documentation for equipment received by the staff and access cards in connection with the employment, and documentation for return of equipment and cards when the employment is terminated. We have inspected training course and competence development plans for the service organization's staff.	No deviations were found.

Control objectives: Physical and Environmental Security

- *To prevent unauthorized physical access to, damage or interruption of the company's premises and information.*
- *To avoid loss, damage, theft or compromising of assets and interruption of the company's assets.*

Kontrolaktivitet	Test udført af BDO	Resultat af test
Physical and Enviromental Security • GlobalConnect A/S has approved processes and contingency plans for the physical security of IT systems against trespassing, destructive impacts from e.g. flooding, fire and other human-caused impacts. • Public access is not allowed close to those systems. • GlobalConnect A/S' equipment is secured against power failure, cabling errors and the like, and maintenance is performed currently. • Sensitive data or software is not removed, and the IT equipment must not be taken outside the area without proper permission from the responsible manager.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - Data Center solutions – Monitoring, Access control, Preventive maintenance, Physical security, Contingency Plan.	The half-yearly control of all open employee access cards, which have not been used for six months, has not been performed as expected. Request forms for temporary access cards were in several cases not completed with sufficient information or were attached as documentation in the Service Management system.

ISO 27001/27002 Compliance

Control objectives: Communication and Operational Management

- *To implement and maintain an adequate level of information security and services in accordance with agreements for third party services.*
- *To maintain integrity and availability of information and information processing equipment.*
- *To ensure protection of information in networks and protection of the underlying infrastructure.*
- *To prevent unauthorized detection, change, removal or destruction of assets or interruption of business activities.*
- *To ensure correct and safe operation of information processing equipment.*
- *To minimize the risk of systems failure.*
- *To prevent interruption of business activities and protect critical business processes against the impact of major crashes in information systems or disasters and to secure a timely restore.*
- *To protect the integrity of software and information.*

Control activity	Test performed by BDO	Result of test
Communication and Operational Management • GlobalConnect A/S has approved processes for operation and maintenance of the IT systems. • A segregation of duties is maintained between development and operation of the IT systems for all important system. • Audits/tests are performed regularly to ensure that the processes described are complied with and that variances are reported. • There are activities concerning handling of capacity measurements and test and acceptance criteria for IT systems. • IDS/IPS controls are performed for all GlobalConnect A/S' IT Data Center operating systems used by OMC. • Backup is performed regularly of all IT systems. • The security, including redundancy, in the IT network and safe handling of media has been implemented. • The exchange IT information is performed in accordance with relevant provisions of the IT security policy. • Activities in the IT systems are logged, including attempts of unauthorised access to the systems.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - General control environment - Dark Fiber solutions - Transmission solutions - Data Center solutions - Internal processes	No deviations were found.

ISO 27001/27002 Compliance

Control objectives: Access Controls

- *To control access to information.*
- *To secure the access of authorized users and prevent unauthorized access to the information systems.*
- *To prevent unauthorized user access and compromising or theft of information and information processing equipment.*
- *To prevent unauthorized access to operating systems.*
- *To prevent unauthorized access to information in business systems.*
- *To secure information when mobile equipment or remote work places are used.*

Control activity	Test performed by BDO	Result of test
Access Controls • Rules have been drawn up for access control. • The responsibility for user access and user responsibilities for the systems has been defined. • GlobalConnect A/S has implemented sufficient network access control to secure access from the outside, including mobile access.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - Internal processes – Logical access, Segregation of duties.	No deviations were found.

Control objectives: Information Security Incident Management and Business Continuity Management

- *To assure that information security incidents and weaknesses relating to information systems are communicated properly to initiate corrective action in time.*
- *To secure a uniform and efficient method for control of information security failures.*
- *To maximize the effect of and minimize disturbances of/in the audit process of information systems.*

Control activity	Test performed by BDO	Result of test
Information Security Incident Management and Business Continuity • All IT security incidents are recorded and dealt with. • GlobalConnect A/S' IT contingency plan is tested and documented, and it is updated at least every second year. • GlobalConnect A/S' IT security is audited in accordance with the standard and approved processes, and documentation is available in this respect.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - General control environment – Threats, Contingency plans. - Dark Fiber solutions – Monitoring, Contingency plan. - Transmission solutions – Monitoring and error handling, Contingency plan. - Data Center solutions – Monitoring, Physical security, Contingency plan.	No deviations were found.

ISO 27001/27002 Compliance		
Control objectives: Compliance • *To avoid breach of legislation, statutory, regulatory or contractual liabilities and security requirements.* • *To ensure that systems fulfill the requirements in the company's security policies and security standards.*		
Control activity	**Test performed by BDO**	**Result of test**
Compliance • GlobalConnect A/S' IT security is audited in accordance with current legislation and recognised standards for information security. • Documentation is available for each audit. • Approved processes are implemented to ensure compliance with current legislation.	We have made inquiries of relevant staff at the service organization. We have inspected documentation that the IT security policy is audited and updated and approved by the management of the service organization as a minimum once a year.	No deviations were found.

ISO 22301 Compliance		
Control objectives: • *To assure maintenance and testing of IT contingency plans for maintenance of a reliable operation of IT systems used.* • *To assure maintenance of the Risk Management plan and recording of all incidents presenting a risk for the daily operation of the solutions.*		
Kontrolaktivitet	**Test udført af BDO**	**Resultat af test**
Approved contingency plan • GlobalConnect A/S has at any time an approved contingency plan for IT, OMC and Housing. • GlobalConnect A/S has at any time an approved 5-year test plan for the contingency plans.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - General control environment – Threats, Contingency plans. - Dark Fiber solutions – Monitoring, Contingency plan. - Transmission solutions – Monitoring and error handling, Contingency plan. - Data Center solutions – Monitoring, Physical security, Contingency plan.	No deviations were found.
Approved and updated IT security policy and analysis • GlobalConnect A/S has at any time an approved IT security policy. • GlobalConnect A/S has at any time an updated risk analysis.	We have made inquiries of relevant staff at the service organization. As regards the work we have performed to test the control activities, we refer to the areas: - General control environment – Threats. - ISO 27001/27002 Compliance – Security Policy.	No deviations were found.
Other matters • The staff involved possess the relevant competences to deal with the contingency. • The processes for operation and monitoring include a clear set of rules for communication in case of critical failure. • There is sufficient documentation in the Service Management system for tests performed of the contingency plan. • There is sufficient documentation in connection with actual cases of contingency.	We have made inquiries of relevant staff at the service organization. For det arbejde vi har udført, for at teste kontrolaktiviteterne, henviser vi til områderne: - General control environment – Threats, Contingency Plans. - Dark Fiber solutions - Monitoring, Repair, Contingency Plan. - Transmission solutions – Monitoring and error handling, Network administration, Contingency plan. - Data Center solutions – Monitoring, Contingency plan.	No deviations were found.

SUPPLEMENTARY INFORMATION FROM GLOBALCONNECT A/S

In order to deal with the differences identified by BDO in the ISAE 3402 report, GlobalConnect A/S will take steps to the following measures.

Action plan		
Control activity	**Result of test**	**Measure**
Access control / Physical and Enviromental Security	The half-yearly control of all open employee access cards, which have not been used for six months, has not been performed as expected. Request forms for temporary access cards were in several cases not completed with sufficient information or were attached as documentation in the Service Management system.	In connection with the designing of a new process for employee access cards, there was an internal misunderstanding as to the responsibility for the task, and the control was therefore by mistake not reviewed. We have now corrected our procedure and it is now clearly shown where the responsibility for review of lists etc. for external and internal access cards that have not been used for a period of six months is placed. We assess that the incident has not compromised our security because we have another procedure to ensure that employee access cards are deleted when employees leave. OMC has in 2016 employed several new people. After having identified an insufficient completion of several forms, we have reviewed the procedure with relevant staff in OMC to ensure that all fields in the form are correctly completed in future and that the form is filed correctly. We will continue to work on digitizing the task to minimize the risk of errors. It is our assessment that this difference has not compromised the security because it is an internal process error.

BDO Statsautoriseret revisionsaktieselskab

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