ISAE 3402 REPORT FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2018 ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO DATA CENTER SOLUTION

GlobalConnect A/S

BDO

CONTENT

AUDITOR’S STATEMENT

INDEPENDENT SERVICE AUDITOR’S ASSURANCE REPORT FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2018 ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO DATA CENTER SOLUTION

To: The Management of GlobalConnect A/S
GlobalConnect A/S’ customers and their auditors

Scope

We have been engaged to report on GlobalConnect A/S’ (the “Service Organisation”) description at pages 5 to 13 of controls related to the operations of Data Center solutions throughout the period from 1 January to 31 December 2018 (the description), and on the design and operation of controls related to the control objectives stated in the description.

The Service Organisation’s Responsibilities

At pages 4 of this report, the Service Organisation has prepared a 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 Organisation is responsible for preparing the description and accompanying statement, including the completeness, accuracy and method of presentation of the description and the statement. The Service Organisation is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

Service Auditor’s Independence and Quality Assurance

We have complied with the independence and other ethical requirements of the “Code of Ethics for Professional Accountants” issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

BDO applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the Service Organisation’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 organisation involves performing procedures to obtain evidence about the disclosures in the service organisation’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 organisation and described at page 4.

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

Limitations of Controls at a Service Organisation

The Service Organisation's description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of the solution that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation 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 in the Service Organisation's statement at page 4. In our opinion, in all material respects:

a. The description fairly presents the controls relating to Data Center solution as designed and implemented throughout the period from 1 January to 31 December 2018; 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 2018; 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 2018.

Description of Tests of Controls

The specific controls tested, and results of those tests are listed at pages 15 to 32.

Intended Users and Purpose

This report is intended only for the service organisation's customers and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 14 February 2019

BDO Statsautoriseret revisionsaktieselskab

Per Sloth
Partner, Head of Risk Assurance
Registered Public Accountant

Lene Yde Poulsen
Director, CISA

GLOBALCONNECT A/S' STATEMENT

GlobalConnect A/S has prepared the following descriptions of services and relevant controls in relation to Data Center solutions.

The description has been prepared for the Service Organisation's customers and their auditors who have a sufficient understanding to consider this description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.

GlobalConnect A/S confirms that the accompanying description fairly presents services and relevant controls in relation to Data Center solution throughout the period from 1 January to 31 December 2018. The criteria used in making this statement were that the accompanying description:

1. Presents how the services and relevant controls in relation to Data Center solutions were designed and implemented, including:
   - The services provided.
   - The procedures within both information technology and manual systems to ensure confidentiality, integrity and availability of systems and data.
   - Relevant control objectives and controls designed to achieve those objectives.
   - Other relevant aspects of control environment, risk assessment process, information systems, communication, control activities and monitoring controls of relevance for the customers' Data Center solution.
2. Includes relevant details of changes to services and relevant controls in relation to Data Center solutions during the period from 1 January to 31 December 2018.
3. Does not omit or distort information relevant to the scope of the services described and the relevant controls relating to Data Center solutions considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of the solution and controls that the individual customer may consider of importance to their special environment.

GlobalConnect A/S confirms that 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 2018. The criteria we used in making this statement were that:

1. The risks that threatened achievement of the control objectives stated in the description were identified.
2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.
3. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 January to 31 December 2018.

Taastrup, 11 February 2019

GlobalConnect A/S

Martin Lippert
CEO

GlobalConnect

GLOBALCONNECT A/S' DESCRIPTION

GENERAL DESCRIPTION OF GLOBALCONNECT

GlobalConnect is provider of Dark Fiber solutions, Transmission solutions, Outsourcing Services (including Cloud services) 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's vision is to be the leading telecom and data communications service provider in Denmark and Northern Germany a key player in the markets where we are operating.

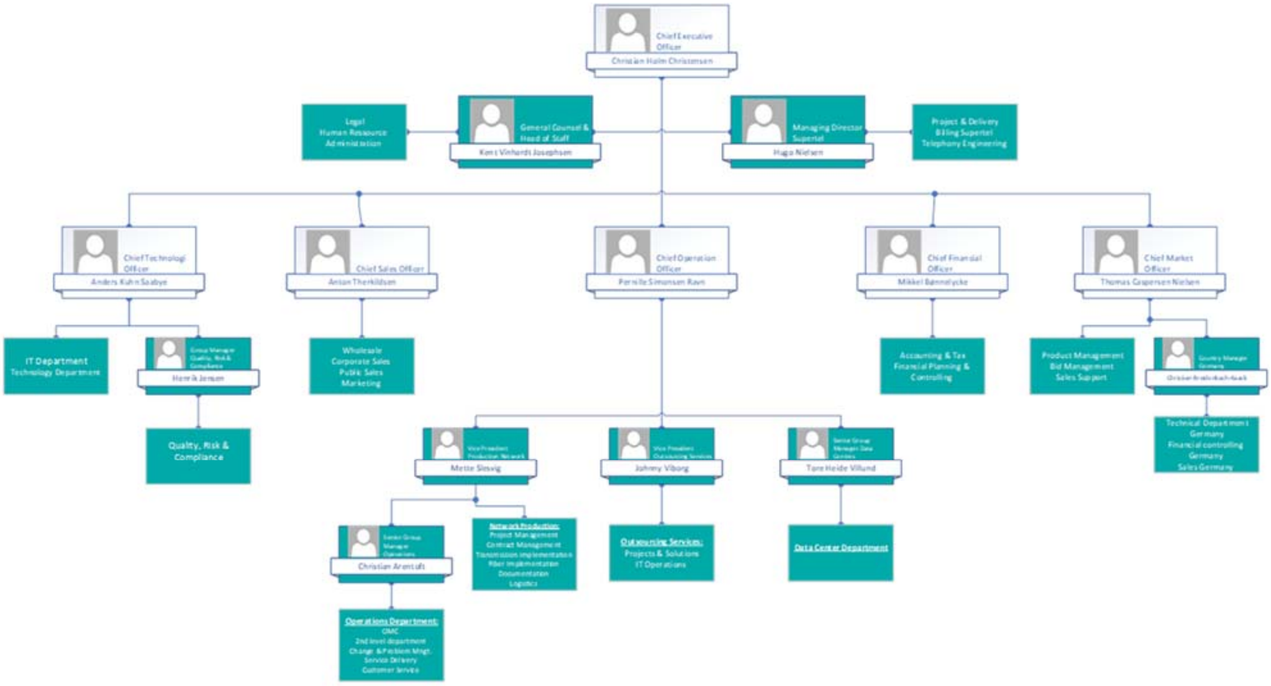
This description comprises services within Data Center solutions. Controls relating to the Dark Fiber and Transmission solutions are covered by a separate ISAE 3402 Type 2 Assurance Report for the period from 1 January to 31 December 2018 on the description on those controls, their design and operating effectives, and are therefore not a part of this description.

GENERAL DESCRIPTION OF THE GLOBALCONNECT'S ORGANISATION

Internal organisation of GlobalConnect:

- A Management consisting of 4 directors who constitute the senior management in the company
- A Sales organisation with offices in Taastrup, Stilling, Odense and Hamburg
- A Product Management and Sales Support department
- A Marketing department
- A Production department with the subdivisions Fiber Implementation, Transmission Implementation, Logistics department, Project Management and Contract Management
- A Data Center department with all Global Connects Data Center operations, maintenance and building activities, located in Taastrup, Stilling and Hamburg
- An Outsourcing department handling design and operation of cloud and outsourcing services
- An Operations department with OMC, 2nd level operations, Infrastructure development, Service delivery department, and a Change Management department
- An IT department with Operations and Support, Business Support Systems and Operations Support system
- Executive functions for Finance, HR, Legal and Administration
- A Quality, Risk & Compliance department
- A number of subsidiaries providing tele-related services, typically based on services purchased from GlobalConnect.

GlobalConnect's organisation August 1, 2018:



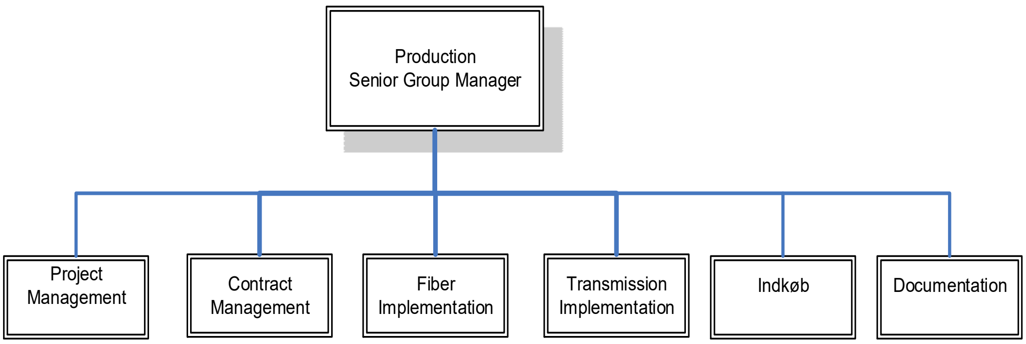
Current description of GlobalConnect organisation.

Production department

GlobalConnect has for organisational 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 organisation

The implementation organisation 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. Approx. 50 people are attached to the implementation organisation.



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

Contract Management is responsible for validation of contracts for the purpose of invoicing and debtor handling.

GlobalConnect

Fiber Implementation - Digging work: charting of trace, examination of existing piping and wiring system and consideration by authorities. The next step is specification of requirements, contracting, management of contractors, supervision 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 drilling work. Splicing of fibers is primarily performed by GlobalConnects staff, however, in case of heavy workloads, subcontractors may be used for splicing of new fiber runs and planned changes of the network.

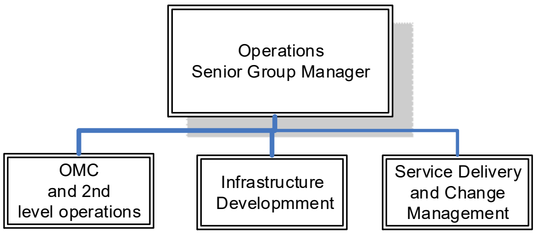
Transmission Implementation – Network element, including specification of requirements, installation of active equipment, quality and testing requirements, tenders and handing-over. Project management, time management, economy, suppliers, responsibility for progress and quality of the assignment, including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

Documentation – documentation of all fibers with relevant connections in the GIS programs Cross, MapInfo and ConnectMaster used in GlobalConnect.

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

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

Operations



Approx. 30 people are attached to Operations which is responsible for the day-to-day operations and monitoring of fiber and transmission network, and data sites and amplifier sites as well as development and maintenance of GlobalConnect's transmission infrastructure. Moreover, Operations is responsible for Quality management, Service management in relation to customers and handling of planned work throughout the organisation.

OMC and 2nd level support – 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 (OMC), which is responsible for the operations.

Infrastructure Development/3rd level support - Responsible for expansion and maintenance of GlobalConnect's backbone network and handling of complex incidents.

Service Delivery and Change Management – Reporting and current service level handling in relation to customers, tests and acceptance of solutions delivered to the customers and general planning and handling of change management (planned work in the network).

Description of the service organisation
In the daytime, 3 - 6 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.

GlobalConnect

Second level support has 6 employees at disposal through our technical organisation. Third level support has 6 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 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 trace, 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.

Description of Quality, Risk & Compliance

The department is responsible for identification and description of quality and information security parameters, maintenance and continuous optimisation of an ISO 9001-based quality management system, implementation of quality and information security parameters in the organisation, including performing and evaluating internal audit. The department is also responsible for contingency training, Risk Management tasks, regulatory requirements relating to information security and corporate social responsibility.

GENERAL DESCRIPTION OF DATA CENTER SOLUTION IN DENMARK AND NORTHERN GERMANY

Data Center solutions are an important element of GlobalConnect's provision of tele services, because Data Center 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 24/7/365.

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

The Data Center solutions are designed with N+1 redundancy on all critical systems, for example power supply secured by redundant UPS and diesel-powered generators. The cooling systems are also redundant. Incidents are recorded in the Service Management System.

The Data Center solutions are placed at the node of the GlobalConnect 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 and ensures that the communication direction can be reversed in case of cable breakdown or breakdown of transmission equipment.

GlobalConnect has Data Centers in both Denmark and Germany

- 20 sites in Taastrup
- 6 sites in Hamburg
- 4 sites in Kolding
- 3 sites in Aarhus
- 1 site in Albertslund
- 1 site in Central Copenhagen
- 1 site in Copenhagen NV
- 1 site in Odense

GlobalConnect

Monitoring of Data Center solutions from an operations center staffed 24 hours a day

GlobalConnects OMC – Operations & Maintenance Centre – in Taastrup monitors closely Data Center solutions, among others by video monitoring of entrances and gates to the areas. The OMC is staffed 24/7/365.

High security is achieved by, among others, personal access control, 24-hour monitoring by OMC, including video monitoring, advanced fire and trespassing alarms. Incidents or alarm, from access control to fluctuations in air temperature, are investigated immediately. Power supply is ensured by redundant UPS and diesel-powered generators, and the cooling systems are also redundant.

GlobalConnect uses a Service Management system for recording and follow-up and documentation of incidents in both internal IT systems and the customer-focused solutions. This increases to a considerable extent the security in handling of errors and breakdowns reported by the customers or which are identified in connection with the 24-hour monitoring.

GENERAL DESCRIPTION OF THE OVERALL CONTROL ENVIRONMENT

GlobalConnects control environment reflects the position Management has taken of the importance of risks, controls and the emphasis that is given to controls in policies, processes, procedures, methods and the organisational structure.

GlobalConnects Q&ISMS is designed to comply with the requirements of the international standard ISO/IEC ISO 27001. The relating control environment for current enhancements and preventive measures is dealt with by QRC under the management of an information security and quality manager. Meetings are held regularly in GlobalConnect's Quality and IT Security Forum (KSU), which includes key employees from different areas in the organisation.

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's Quality and IT security Forum (Kvalitets- og IT-sikkerhedsforum (KSF)). This forum includes 2 directors, an assistant director and Senior Group Managers from Operations and GlobalConnect-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.

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

RISK ASSESSMENT

An annual risk assessment is carried out and input for this assessment is obtained from all levels in the organisation and by statutory and regulatory authority requirements. The process is facilitated by a quality and security committee consisting of executive staff from relevant departments. The assessment is presented to the company's senior management for approval. A contingency plan is also prepared annually which reflects the existing threat scenario.

Risk assessments are based on the implementation guidelines in the international standard ISO27002.

GlobalConnect performs current activities which are to:

1. Analyse and chart GlobalConnect overall infrastructure (transmission and cable routes, buildings, etc.),
2. Identify the threats constituting the most significant risks,
3. Identify, select and prioritise the state of alert for those risks.

The likelihood and consequence of the threats are reassessed based on the information existing at the present time. This reflects, in combination, the threat level. When the threat level is low, the need for security measures is lower than when the threat level is high. When the threat level has been determined, it is assessed to which extent the security environment considers the relevant threat level and it can be deduced here from how high the relevant remaining risk is.

The day-to-day Management of GlobalConnect decides on the basis of the risk assessment whether an identified risk can be accepted, is to be reduced or whether insurance is required based on selected risks.

Critical risks are examined to assess vulnerabilities in relation to the preventive measures already taken to meet the threats. As regards the risks that are considered unacceptable, an overall action plan has been prepared to deal with risks.

Preventive and enhancing measures are implemented regularly to limit known threats and vulnerabilities.

For a description of control objectives and controls for risk assessment in relation to Data Center solutions, we refer to A.4 under control objectives, controls, tests and results of tests which are an integral part of this description.

CONTROL OBJECTIVES AND CONTROLS FOR DATA CENTER SOLUTIONS

Control objectives and controls for Data Center solutions are determined for the areas listed below in accordance with the overall control environment, based on the international standard ISO/IEC ISO 27001/27002. The description of control objectives and controls for these areas under control objectives, controls, tests and results of tests is an integral part of this description.

- A.5: Information security policies
- A.6: Organisation of information security
- A.7: Human resource security
- A.9: Access control
- A.11: Physical and environmental security
- A.12: Operations security
- A.16: Information security incident management
- A.17: Information security aspects of business continuity management

A.5 Information security policies

GlobalConnect has drawn up a formal information security policy. This is handed out in connection with employment and, moreover, all employees are under an obligation to keep themselves updated annually in relation to information security policies and the relevant manuals. Finally, our suppliers/business partners are also familiar with this when obtaining non-disclosure agreements. The information security policy is reassessed annually by Management.

A.6 Organisation of information security

GlobalConnect has implemented controls to ensure a general management of the information security including a delegation of responsibilities and handling of material risks in accordance with the requirements of the company's Management.

Management's obligations in relation to information security
Management takes an active part in the information security in the organisation. The formal responsibility, including approval of the information security policy, is also that of the CEO.

Coordination of the information security
Activities to safeguard the information security are considered in a cross-organisational quality and security committee (KSU) with participants from all relevant departments.

GlobalConnect

Placing of responsibility for information security
All areas of responsibility for the information security are described in GlobalConnect's security policy which clearly describes where the responsibility is placed in relation to information security and the contingency planning.

A.7 Human resource security

GlobalConnect has implemented controls to ensure that suitable background checks have been made of employees and that these are conscious of their tasks and responsibilities in relation to information security.

Some customers require security clearance of our employees. A condition for the access to customers' IT environment is as a minimum an unblemished criminal record and, if required by the customers, a PET clearance and/or and FE clearance. PET and FE clearances are renewed by the issuing authority at predefined intervals.

Management's responsibility
As regards employees, they commit themselves, at their employment, to comply with the company's policies, including the security policy.

Awareness of information security, education and training
As regards employees, they are informed of all material changes to applicable policies and relevant procedures. This is done partly at the monthly meetings in the Quality and Security Forum and partly at staff meetings.

Non-disclosure agreements
Confidentiality is part of the employment contracts. For a few customers there are special non-disclosure and confidentiality agreements and other security provisions for the employees working with the customers' IT environments. Moreover, an overview has been prepared of all laws, requirements and security circulars that GlobalConnect must comply with. The overview is maintained by periodical reviews.

Obligations relating to resignation
General employment conditions, including conditions in relation to end of employment, are described in the employee's employment contract and the relating solemn declaration. Moreover, there is a formal procedure for resignation which must be followed by the immediate manager. The HR manager is the ultimate responsible in this respect.

Return of equipment
All employees are to return all received material when the employment contract ends. This is done through a workflow placed at the HR department.

Closing down of access rights
GlobalConnect's formal HR procedures ensure that all rights and physical access are withdrawn when an employment ends. This is done through a workflow placed in the HR department Accesses are reviewed periodically as part of our quality management system.

A.9 Access control

GlobalConnect has implemented controls to ensure that access to systems and data are granted through a documented process in accordance with a relevant work-related need and is closed down when the relevant access is no longer necessary.

User creation
GlobalConnect has procedures for creation and closing down of users which are placed in the HR department.

Extended rights
All rights are managed on the basis of the employees' roles and are checked regularly in our quality management system.

GlobalConnect

Management of password

Granting of passwords is subject to a number of rules which are set out in our Active Directory.

A.11 Physical and environment security

GlobalConnects OMC in Taastrup monitors all data centres, among others also video monitoring of entrances and gates to the areas. The OMC is staffed 24/7/365.

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 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.

All Data Centers, including cooling systems, generators, 48-Volt-systems, UPS, fire systems, etc. are subject to periodical service checks by GlobalConnect's own technicians and by external service providers.

A.12 Operations security

GlobalConnect uses a Service Management System for recording and follow-up and documentation of all changes in both internal IT systems and the customer-focused solutions within data center solutions. This enhances to a considerable extent the security in handling of errors and breakdown reported by the customers or identified in connection with the 24-hour monitoring.

OMC opens an error report in the Service Management System on all errors with a reference number which is used throughout the following error handling process.

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 in this respect are considered 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 conditions the work is reported as completed in the Service Management System.

GlobalConnect uses Frontsafe as provider of all back-up of the operating systems. GlobalConnect verifies that Frontsafe has documented its controls in an ISAE 3402 auditor's report which is hereafter assessed with respect to compliance with GlobalConnect's requirements for back-up.

A.16 Information security incident management

GlobalConnect has implemented controls to ensure that security incidents are dealt with on a timely basis and that there is follow-up hereon.

Processes and procedures have been implemented for handling of security incidents to ensure a uniform and effective method to manage information security incidents, including communication on security incidents and weaknesses which are documented in Service Management System. Management of security incidents and breakdown follows predetermined procedures defined in GlobalConnect's Q&ISMS' paragraph on incidents and crisis management.

All security incidents are handled in the Service Management System and in accordance with established procedures.

A.17 Information security aspects of business continuity management

GlobalConnect has and maintains contingency plans. The plans set out the responsibility for maintaining an optimal operating reliability, including response time for different levels of critical errors, the escalation process, the process for handling crisis situations and communication with customers and the media in such cases.

GlobalConnect

The plans describe generally the specifications of the installed equipment for power supply, emergency generator, UPS, cooling, fire extinction, alarm system and access control and the activities carried out to maintain those systems for the purpose of current prevention and improvement.

Contingency plans are prepared for Data Center which are updated at least every second year. There is moreover an approved plan for testing of these plans which is applicable for five years ahead and which ensures business continuance in case of security incidents. The testing is documented in the Service Management System.

CHANGES TO SERVICES AND RELATING CONTROLS

In the period from 1 January to 31 December 2018 no material changes were made to GlobalConnect's services within Data Center solutions and relating controls.

CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

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

In the test schedule, we have described the tests performed, which were assessed as necessary in order to obtain a high degree of assurance that the stated control objectives were achieved, and the related controls operated effectively during the period from 1 January to 31 December 2018.

Testing the design and implementation of the controls is carried out by inquiries, inspection, observation and re-performance.

Type	Description
Inquiry	Interviews of relevant personnel at GlobalConnect A/S have been performed for all significant control activities. The purpose of the interviews 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, authorisations 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 is implemented.
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 an independent auditor received an ISAE 3402 report for the period from 1 October 2017 to 30 September 2018 on technical and organisational security measures relating to operation of Cloud Backup services. This service sub-organisation's relevant control objectives and related controls are not included in GlobalConnect A/S' description of services and relevant controls related to operation of Data Center solutions. Accordingly, we have solely assessed the report and tested the controls at GlobalConnect A/S that monitor the operating effectiveness of the service sub-organisation's controls.

A.4: Risk assessment

Control objective

- *To ensure that a risk assessment is performed annually to form basis for commercially founded implementations.*

Control activity	Test performed by BDO	Result of test
Risk assessment • A risk assessment is performed annually which is approved by management. The risk assessment is a part of the work with GlobalConnect's information security management system (ISMS).	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's information security policy, information security rules, and information security manual. We observed that the overall risk assessment is part of the work with the information security management system. We have inspected the service organisation's risk assessment. We observed that meetings are held regularly in the service organisation's quality and security forum, and we have inspected selected minutes of meetings. We observed that the purpose of the meetings is to ensure maintenance, raising and embedding of information security, including current assessment of threats and risks.	No deviations identified.

A.5: Information security policies
Guidelines for management of information security

Control objective

- *To provide guidelines for and support the information security in accordance with business requirements and relevant laws and regulations.*

Control activity	Test performed by BDO	Result of test
Policies for information security • Management sets out and approves policies for information security which after approval are published and communicated to staff and relevant external parties.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's information security policy, information security rules, and information security manual. We observed that the information security policy has been designed in accordance with ISO 27001/27002. We have inspected the service organisation's terms of reference for the quality and security forum set up, including procedures to ensure approval by management and communication within the organisation. We have inspected the information security policy and observed that this has been signed by the management. We observed that the information security policy is communicated to employees and relevant external business partners and we have inspected relevant documentation.	No deviations identified.
Review of policies for information security • GlobalConnect has prepared and implemented a procedure to ensure periodical review of the information security policy. • A written information security policy has been drawn up which is reassessed annually. • The information security policy is approved by management.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's audit plan for review of information security policy, information security rules, and information security manual. We have observed that the determined audit plan is followed, including that the information security policy is reviewed and reassessed. We have inspected relevant documentation. We observed that the information security policy has been approved and signed by management. We have inspected relevant documentation.	No deviations identified.

A.6: Organisation of information security
Internal organisation

Control objectives
- *To establish a managerial basis to enable initiation and management of the implementation and operation of the information security in the organisation.*
- *To safeguard remote workplaces and the use of mobile equipment.*

Control activity	Test performed by BDO	Result of test
Roles and responsibilities for information security • The responsibility for the information security in GlobalConnect lies with the management. • Management has appointed a cross-organisational Quality and Security Forum which considers activities relating to safeguarding of the information security. • Management has designated a Quality and Security Manager who has the overall responsibility for handling the information security.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's information security policy, information security rules, and information security manual and overview of the in-house organisation of the information security. We have inspected the service organisation's terms of reference for the quality and security forum set up, procedure for the quality and security work, and the quality manual, including document handling. We observed that meetings are held regularly in the service organisation's quality and security forum, and we have inspected selected minutes of meetings. We observed that the purpose of the meetings is to ensure maintenance, raising and embedding of information security.	No deviations identified.

A.7: Human resource security
Before employment, during employment and when employment ends or is changed

Control objectives
- *To ensure that employees and contracting parties understand their responsibilities and are suited for the roles they are intended for.*
- *To ensure that employees and contracting parties are conscious of and fulfil their information security responsibilities.*
- *To protect the organisation's interests as part of the change or end of the employment.*

Control activity	Test performed by BDO	Result of test
Before employment • A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee. • When the customer or the task requires security clearance, this is obtained for the relevant employees in accordance with the relevant procedure for this purpose.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedure for employment and departure of staff. We observed that a background check is made as part of the employment process, and we have inspected the approved employment contract template. We have inspected the form to be used for new employees which among others contain information on the areas to which the individual employees are to have access, to the programmes and rights the employee should be granted. We observed that the form is issued by HR and approved by the immediate manager. We have inspected an overview of new employees in 2018, and we have by random sampling selected and inspected documentation for new employees which follows the service organisation's procedures in this respect, including creation of employees in systems. We have inspected a list of the employees who have obtained security clearance from the Danish Defence Intelligence Service and from PET, and we observed the process for obtaining and maintaining these security clearances.	No deviations identified.
During employment • Employees at GlobalConnect are currently informed of information security matters and potential threats in relation to their tasks. • Employees at GlobalConnect declare at the start of employment that they have read and accept the information security policy and the manual.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's intranet. We have observed that the employees at the service organisation are kept updated on information security matters and any threats relating to their tasks.	No deviations identified.

A.7: Human resource security
Before employment, during employment and when employment ends or is changed

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suited for the roles they are intended for.*
- *To ensure that employees and contracting parties are conscious of and fulfil their information security responsibilities.*
- *To protect the organisation's interests as part of the change or end of the employment.*

Control activity	Test performed by BDO	Result of test
	We have inspected publications to the employees on selected subjects within information security and data protection legislation. We have observed that the publications have been included in information campaigns, etc.	
Non-disclosure and confidentiality agreements • All employees working with confidential data – including personal data – have signed a non-disclosure agreement.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's process for employment of new staff and approved employment contract template. We observed that the employment contract includes conditions on confidentiality, applicable during employment and at the end of employment and for both in-house and customer-related data. We have inspected randomly selected employment contracts and observed that the conditions for confidentiality are described and that the employment contract is signed by the employee.	No deviations identified.
End or change of the employment • After the end or change of the employment, accesses and rights are withdrawn or changed in accordance with the functional need in this respect. • After the end of the employment, equipment received by the leaving employee is returned. • After the end of the employment, HR ensures that the procedure for departure is complied with.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedure for employment and resignation of employees. We have inspected the form used in connection with departure. We observed that OMC/IT and the employee sign the resignation form for closing of access cards and return of the service organisation's physical equipment. The departure form is kept in the HR manager's physical files.	No deviations identified.

A.7: Human resource security
Before employment, during employment and when employment ends or is changed

Control objectives

- *To ensure that employees and contracting parties understand their responsibilities and are suited for the roles they are intended for.*
- *To ensure that employees and contracting parties are conscious of and fulfil their information security responsibilities.*
- *To protect the organisation's interests as part of the change or end of the employment.*

Control activity	Test performed by BDO	Result of test
	We have inspected overview of employees who left in 2018, and we inspected resignation form for randomly selected employees, who have left, which follows the service organisation's procedures in this respect, including closing down of employees in systems.	

A.9: Access controls
Business requirements for access management, administration of user access, responsibility of users and management of systems and application access

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To make users responsible for safeguarding their authentication information.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Policy for access management • Processes and procedures have been adopted to manage access and restrictions to systems and data based on business and functional requirements. • All access and changes to access to systems and data follow the adopted processes and procedures.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedure for employment and departure of employees, procedure for access control to physical locations and systems and procedure for escorted access to the service organisation's data centers. Based on inspection of documentation for the following areas under A.9, we observed that the adopted processes and procedures are complied with.	No deviations identified.
User registration and deregistration • GlobalConnect has implemented and follows the process for creation and deregistration of users in systems.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedure for employment and departure of employees. We have inspected the form to be completed for new employees and the form relating to departure. We have inspected overview of new employees and employees who left in 2018, and we have randomly selected and inspected documentation for new employees and employees, who have left, which follows the service organisation's procedures in this respect, including creation and closing down of employees in systems.	No deviations identified.

A.9: Access controls
Business requirements for access management, administration of user access, responsibility of users and management of systems and application access

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To make users responsible for safeguarding their authentication information.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
Granting, adjustment and withdrawal of access rights • GlobalConnect has implemented a procedure for granting of user access for the purpose of granting access rights for all types of users to all systems and services. • GlobalConnect has implemented a process for withdrawal or adjustment of access rights, including deletion of an employee's access when moving or leaving.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedure for employment and departure of employees. We have inspected the form to be completed for employees which among others contain information on the areas to which the individual employee should have access and the programmes and rights that should be granted to the employee. We observed that the form is issued by HR and approved by the immediate manager. We have inspected access control lists (whitelists) for a sample of the service organisation's customers. We have inspected the departure form used. We have inspected overview of new employees and employees who left in 2018, and we have randomly selected and inspected documentation for new employees and employees, who have left, which follows the service organisation's procedures in this respect, including granting of access to systems and services.	No deviations identified.
Management of privileged access rights • GlobalConnect has implemented granting of administrative access to entities according to the functional need which is authorised. • GlobalConnect has implemented logging of accesses with privileged accounts (administrative rights).	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedure for employment and departure of employees.	No deviations identified.

A.9: Access controls
Business requirements for access management, administration of user access, responsibility of users and management of systems and application access

Control objectives

- *To restrict access to information and information processing facilities.*
- *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- *To make users responsible for safeguarding their authentication information.*
- *To prevent unauthorised access to systems and applications.*

Control activity	Test performed by BDO	Result of test
	We have inspected the form to be completed for employees which among others contain information on the areas to which the individual employee should have access and the programmes and rights that should be granted to the employee, including granting of administrative access. We observed that the form is issued by HR and approved by the immediate manager. We have inspected overview of new employees in 2018, and we have randomly selected and inspected documentation for new employees, which follows the service organisation's procedures in this respect, including granting of access to systems and services. We have inspected the audit policy in the service organisation's network operating system which ensures logging of access by users with privileged/administrative rights.	
Management of passwords to users • GlobalConnect has implemented a process and rules for granting and management of passwords. • GlobalConnect has implemented rules for establishment of passwords which must be followed by all employees.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's information security rules and information security manual for use of passwords, including procedure for user access to IT systems. We have inspected the password policy and the audit policy in the service organisation's network operating system. We have observed that management of passwords has been set up. We have inspected extract from user set-up from the service organisation's Active Directory and reperformed the control for passwords. We observed that the password rules are followed by all employees.	No deviations identified.

A.11: Physical and environmental security
Secure areas and equipment

Control objectives

- *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.*
- *To avoid loss, damage, theft or compromising of assets and business interruption in the organisation.*

Control activity	Test performed by BDO	Result of test
Physical perimeter safety guarding • The established physical perimeter safety guarding is in agreement with the adopted security requirements.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedures for access control and escorted access to locations. We have inspected the physical perimeter safe guarding relating to office buildings and selected data centers. We observed, by random sampling, the handling of guest cards and we inspected the documentation of the selected samples.	No deviations identified.
Physical access control • Access controls have been established which guard against the probability of unauthorised physical access to, damage or interruption of GC's premises and information – including ensuring that only authorised persons have access. • Activities are recorded in the access control system OMC. • Half-yearly review has been made of external access cards that have not been used within the last six months. • Half-yearly review has been made of internal access cards that have not been used within the last six months • Test control of selected access points to ensure that the right persons have the right accesses.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedures for access control and escorted access to locations and procedure for access control in connection with employment and departure of employees. We observed that the employees' physical access rights are granted on the basis of a work-related need, and that the management of these access rights is made in OMC. We have inspected documentation in this respect. We have observed that control is carried out monthly to ensure that the access of employees, who have left, has been closed down. We have selected a sample and inspected this. We have inspected randomly selected creations and closing down of access for employees. We have inspected extract from the access control system and inspected key list of physical keys. We observed the implemented access controls. We observed procedure for escorted access and inspected documentation in this respect in Service Management System by random sampling.	No deviations identified.

A.11: Physical and environmental security
Secure areas and equipment

Control objectives

- *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.*
- *To avoid loss, damage, theft or compromising of assets and business interruption in the organisation.*

Control activity	Test performed by BDO	Result of test
	We have observed procedure for customers' and suppliers' access, including access as a guest or access to administrative areas. We have inspected selected creations and closing down of customers' and suppliers' access. We have inspected extracts from the access control systems. We have observed the established access controls. We have inspected the service organisation's half-yearly review of external and internal access cards, which have not been used within the last six months, and the test control of access points.	

Protection against external and environmental threats
• GlobalConnect complies with specified requirements for physical security for data center solutions including:
  • Building
  • Floors
  • Foot-prints
  • Climate
  • Power supply
  • Access
  • Alarm monitoring
  • Fire extinction
  • Cabling
	We have interviewed relevant personnel at the service organisation.
	
	We have inspected the service organisation's information security policy, information security rules and information security manual.
	
	We have inspected and observed the physical security measures for selected data centers. We observed that the physical security measures are based on specific risk assessments for the individual data centers.
	
	We observed that the data centers are located in fenced-in industrial areas to which key cards or code to doors and gates are required. We observed that the entrance areas are camera monitored.
	
	We have observed that doors to the data centers are fireproof, and that the ceilings are coated with fire-resistant material. We observed that automated fire control equipment is established in the data centers, that the floors are elevated and coated with antistatic flooring, and that humidity sensors are installed under the elevated floors.
		No deviations identified.

A.11: Physical and environmental security Secure areas and equipment		
Control objectives • *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.* • *To avoid loss, damage, theft or compromising of assets and business interruption in the organisation.*		
Control activity	**Test performed by BDO**	**Result of test**
	We have observed that redundant cooling systems are installed in the data centers which are serviced and maintained annually. We have observed that alarms are installed for water, humidity, smoke and temperature, and that all alarms go to OMC. We have observed that power intake is attached to each data center and that the power and fiber are drawn under the elevated floor or placed in cable trays under the roof.	
Work in secure areas • GlobalConnect has established monitoring in data centers and suitable safeguarding of guidelines for activities and work in the areas.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's information security policy, information security rules and information security manual. We have inspected selected physical data centers and observed that, with respect to the data centers located in physical buildings, camera monitoring is installed, and that the data centers are monitored by OMC. We observed that the walking areas in the data centers are monitored 24 hours a day. We have inspected the service organisation's physical access control and protection measures against external and environmental threats.	No deviations identified.
Placing and protection of equipment • GlobalConnect has established suitable measures to prevent unauthorised access to customers' systems, data and information.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedures for access control and escorted access to locations and procedure for access control relating to new employments and departures of employees.	No deviations identified.

A.11: Physical and environmental security
Secure areas and equipment

Control objectives

- *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.*
- *To avoid loss, damage, theft or compromising of assets and business interruption in the organisation.*

Control activity	Test performed by BDO	Result of test
	We have inspected selected physical data centers and observed that entry to a data center requires access card with a personal code, and that the entrance and walking areas are camera monitored and 24 hours' monitored. We have inspected the service organisation's physical access control and protection measures against external and environmental threats.	
Underlying supplies (supply reliability) • GC has established and maintains equipment to ensure that the consequences of business interruption are mitigated. • A check is made with respect established ventilation, cable trays, etc. according to a fixed template for inspection (maintenance report). • GlobalConnect reviews maintenance reports.	We have interviewed relevant personnel at the service organisation. We have inspected the procedure for planned work for the individual data centers in the Service Management System. We have inspected documentation for randomly selected monthly maintenance reports from data centers. We have inspected list of external providers and randomly inspected service and maintenance reports from these providers relating to the implemented security measures in data centers and repeater sites.	No deviations identified.
Maintenance of equipment • GlobalConnect performs monthly preventive inspection of data center facilities. The result of these inspections is documented in completed schedules. • GlobalConnect has established periodical maintenance of fire extinction systems, cooling systems and generators in data centers of external service organisations.	We have interviewed relevant personnel and inspected descriptions of procedures, internal controls and standard agreements. We have inspected the procedure for planned work for the individual data centers in the Service Management System. We have inspected documentation for randomly selected monthly reports from data centers.	No exceptions found.

A.11: Physical and environmental security
Secure areas and equipment

Control objectives

- *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.*
- *To avoid loss, damage, theft or compromising of assets and business interruption in the organisation.*

Control activity	Test performed by BDO	Result of test
	We have inspected list of external providers. We have observed that the service provider has signed annual service agreements, for check of cooling systems, diesel generator, UPS system, and the automated fire control equipment. We have inspected the service agreements. We have randomly inspected service and maintenance reports from providers relating to the implemented security measures in data centers.	

A.12: Operations security
Operating procedures, change management, backup, and monitoring

Control objectives

- *To ensure correct and reliable operation of information processing facilities.*
- *To ensure that information and information processing facilities are protected against malware.*
- *To record incidents and obtain evidence.*
- *To ensure the integrity of operating systems.*
- *To prevent exploitation of technical vulnerabilities*
- *To minimise the impact of audit activities on operating systems.*

Control activity	Test performed by BDO	Result of test
Back-up • GlobalConnect uses third-party provider (Frontsafe A/S) for all back-up of the operating systems. • Frontsafe A/S has documented its controls in an ISAE 3402 auditor's report which GlobalConnect reviews annually.	We have interviewed relevant personnel at the service organisation. We have inspected Service Level Agreement from Frontsafe A/S relating to Cloud Backup services. We observed that the service organisation has obtained independent auditor's ISAE 3402 report for the period from 1 October to 30 September 2018 on technical and organisational security measures relating to the operation of Cloud Backup services. We have inspected the above ISAE 3402 report.	No deviations identified.
Change management • GlobalConnect has established a process for management of changes in data centers which is carried out according to defined routines for change management. • Changes and management hereof are documented in Service Management System. • Customers are warned according to a defined time schedule before the change to ensure least possible inconvenience for the customers.	We have interviewed relevant personnel at the service organisation. We have inspected procedure for implementation and operation of data centers and procedure for change management, including instructions and check lists. We observed that planned work is created in Service Management System, and that OMC is responsible for the change management, including warning of the relevant customers, follow-up on work started and documentation of changes made. We have inspected the Service Management System as documentation for our observation. We have inspected overview of planned work for the period from 1 January to 30 April 2018, when these were managed in a spreadsheet. We have inspected extract from Service Management System of planned work for the period from 1 April to 31 December 2018.	No deviations identified.

A.12: Operations security
Operating procedures, change management, backup, and monitoring

Control objectives

- *To ensure correct and reliable operation of information processing facilities.*
- *To ensure that information and information processing facilities are protected against malware.*
- *To record incidents and obtain evidence.*
- *To ensure the integrity of operating systems.*
- *To prevent exploitation of technical vulnerabilities*
- *To minimise the impact of audit activities on operating systems.*

Control activity	Test performed by BDO	Result of test
	We have inspected documentation of randomly selected planned work and observed the change management process, including warning of customers and completion of the work before the deadline determined.	
Incident logging • Recording and handling of all relevant incidents have been established including attempts of unauthorised access to the systems. • Network is monitored with software tools. Alarms have been set up which notify in case of network errors. • All data centers are monitored by OMC, 24/7/365, and all incidents or alarm, from are examined immediately. • An error report is opened in Service Management System on all errors with a reference number, which is used throughout the following error handling process.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedures for monitoring of data center solutions, including procedures and guidelines for incident management, crisis management of critical errors and emergency preparedness. We observed that monitoring in OMC is made in the systems and visually on screens, and that the implemented procedures and guidelines are followed, including recording of incidents. We observed that incidents are recorded in Service Management System. We have inspected extracts from this system of all incidents happened and created in 2018 in the category Data Center solution. We have inspected randomly selected incidents in Service Management System with the priority critical or high, and observed that response times are met. We have inspected procedure for escalation of critical errors and observed that OMC follows the procedures. We have inspected monthly reports from OMC.	No deviations identified.

A.16: Information security incident management		
Control objective • *To ensure a uniform and effective method of managing information security incidents, including communication of security incidents and weaknesses.*		
Control activity	**Test performed by BDO**	**Result of test**
Handling of information security incidents • All security incidents are handled in Service Management System and in accordance with established procedures.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's information security policy and information security rules, and procedures for handling of security incidents, including procedures and guidelines for escalation process, crisis management of critical errors and emergency preparedness. We observed that incidents are recorded in Service Management System. We have inspected extracts from this system of all incidents happened and created in 2018. We have inspected randomly selected incidents in Service Management System with the priority critical or high. We have inspected the procedure for escalation of critical errors and observed that OMC follows the procedure.	No deviations identified.
Reporting of information security incidents: • Processes and procedures have been established for handling of security incidents to ensure a uniform and effective method of managing information security incidents, including communication of security incidents and weaknesses which are documented in Service Management System. • Processes and procedures have been established to ensure recording and handling of security incidents by the right employees.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's procedures and guidelines for incident management, crisis management of critical errors and emergency preparedness. We observed that incidents are recorded in Service Management System and that the management of the incident is supported by this system, including assignment of the security incident to the right employee, and communication and reporting. We have inspected randomly selected incidents in Service Management System with the priority critical or high. We have observed that the implemented procedures are followed.	No deviations identified.

A.17: Information security aspects of business continuity management
Information security contingency and redundancy

Control objective

- *The information security continuity must be embedded in the organisation's management systems for disaster recovery, contingency and restore management.*
- *To ensure access to information processing facilities.*

Control activity	Test performed by BDO	Result of test
Implementation of information security continuity • Contingency plans are prepared for Data centers to ensure business continuance in connection with security incidents, which are applicable for five years ahead. • The contingency plans are updated periodically.	We have interviewed relevant personnel at the service organisation. We have inspected the service organisation's overall risk assessment and the relating contingency plans and procedures. We have also inspected the procedure for OMC incident management and procedure for crisis management and emergency preparedness. We observed that the service organisation currently updates its contingency plans based on risk assessments, and that updating is made minimum every second year. We have inspected that the contingency plans for Operations and Data centers most recently were updated in March 2017, and that they are applicable until 2023.	No deviations identified.
Verify, review and evaluate the information security continuity • GlobalConnect has established periodical testing of contingency plans for the purpose of ensuring that the contingency plans are up-to-date and effective in critical situations. • Contingency tests are documented by reports from testing.	We have interviewed relevant personnel at the service organisation. ´ We have inspected the service organisation's overall risk assessment and the relating contingency plans and procedures, including procedures for testing of contingency plans. We have inspected the service organisation's plan for test of the contingency plans running from 2018 to 2023. We observed that the service organisation has carried out the planned testing of the contingency plan according to the plan. We have inspected the documentation for the testing which refers to the recordings in Service Management System. We observed that any comments are subject to follow-up or proposed improvements in the service organisation's quality and security forum.	No deviations identified.

BDO Statsautoriseret revisionsaktieselskab

Havneholmen 29
DK-1561 Copenhagen V
CVR no. 20 22 26 70