# GLOBALCONNECT A/S

**INDEPENDENT SERVICE AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2020 ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO DATA CENTER SOLUTIONS IN DENMARK AND GERMANY**

BDO

# CONTENTS

# INDEPENDENT SERVICE AUDITOR'S REPORT

**INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 JANUARY TO 31 DECEMBER 2020 ON THE DESCRIPTION OF CONTROLS, THEIR DESIGN AND OPERATING EFFECTIVENESS RELATING TO DATA CENTER SOLUTIONS IN DENMARK AND GERMANY**

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' (Service Organisation) description at pages 6 to 15 of controls related to the operations of Data Center solutions in Denmark and Germany throughout the period from 1 January to 31 December 2020, and on the design and operation of controls related to the control objectives stated in the description.

## Service Organisation's Responsibilities

The Service Organisation is responsible for preparing statement at pages 4 to 5 and the accompanying description, including the completeness, accuracy and method of presentation of the statement and the description. The Service Organisation is responsible for providing the services covered by the description; stating the control objectives; and 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.

We apply 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.

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, 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 to 5.

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 Data Center solutions 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 to 5. In our opinion, in all material respects:

a. The description fairly presents the controls relating to Data Center solutions in Denmark and Germany as designed and implemented throughout the period from 1 January to 31 December 2020; 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 2020; 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 2020.

## Description of Tests of Controls

The specific controls tested, and results of those tests are listed at pages 17 to 36.

## 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, 30 January 2021

**BDO Statsautoriseret revisionsaktieselskab**

Claus Bonde Hansen
Senior Partner State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA

# GLOBALCONNECT A/S' STATEMENT

GlobalConnect A/S has prepared the following descriptions of controls relating to Data Center solutions in Denmark and Germany.

The description has been prepared for GlobalConnect A/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 controls in relation to Data Center solutions in Denmark and Germany throughout the period from 1 January to 31 December 2020. 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 in Denmark and Germany 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 solutions.

2. Includes relevant details of changes to controls in relation to Data Center solutions during the period from 1 January to 31 December 2020.

3. Does not omit or distort information relevant to the scope of the controls described in relation to 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 Data Center solutions 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 2020. 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 2020.

Taastrup, 28 January 2021

**GlobalConnect A/S**

Louise Hahn
Country CEO DK & Germany

# GLOBALCONNECT A/S' DESCRIPTION

## GENERAL DESCRIPTION OF GLOBALCONNECT A/S

GlobalConnect A/S (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 and a key player in the markets where we are operating.
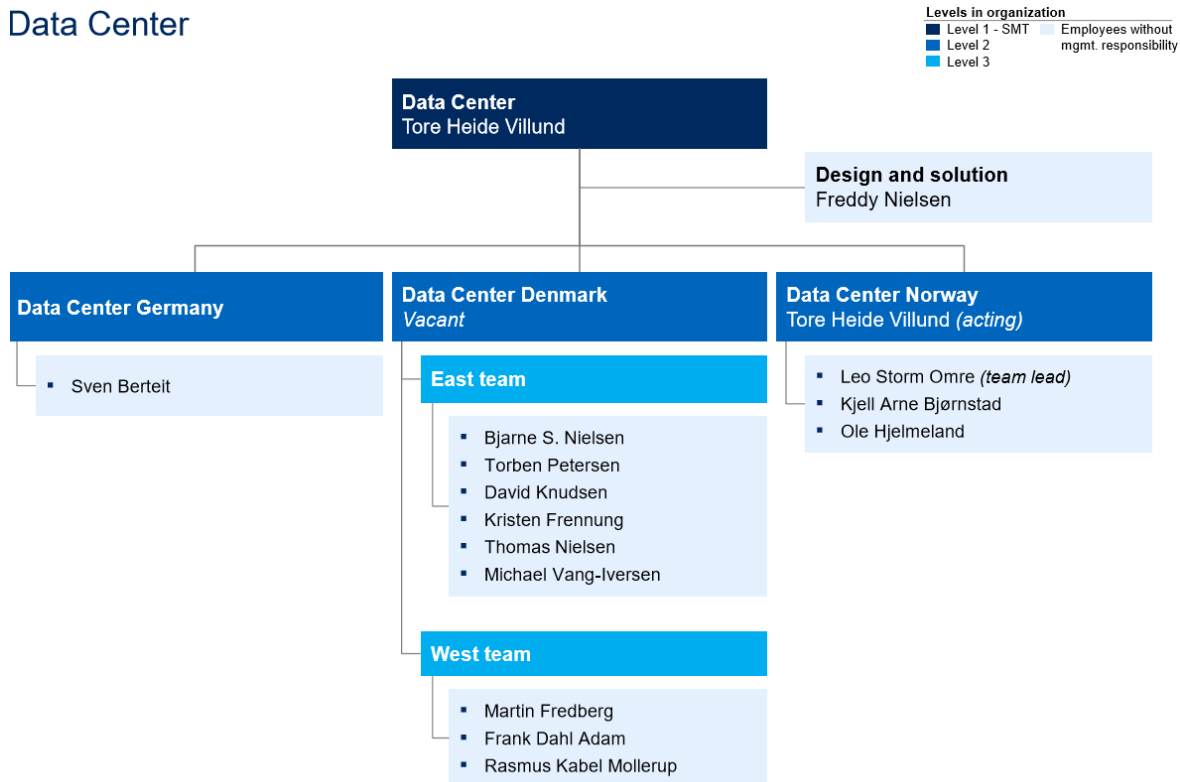
This description comprises services within Data Center solutions in Denmark and Germany. Controls relating to the Dark Fiber and Transmission solutions are covered by a separate ISAE 3402 Type II Assurance Report for the period from 1 January to 31 December 2020 on the description on those controls, their design and operating effectives, and are therefore not a part of this description.

## GENERAL DESCRIPTION OF GLOBALCONNECT'S ORGANISATION

Internal organisation of GlobalConnect:

- A Management consisting of 5 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 Customer Care, 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.

## Data Center

**Levels in organization**
- Level 1 - SMT
- Level 2
- Level 3
- Employees without mgmt. responsibility

**Data Center**
Tore Heide Villund

**Design and solution**
Freddy Nielsen

**Data Center Germany**
- Sven Berteit

**Data Center Denmark**
*Vacant*

**East team**
- Bjarne S. Nielsen
- Torben Petersen
- David Knudsen
- Kristen Frennung
- Thomas Nielsen
- Michael Vang-Iversen

**West team**
- Martin Fredberg
- Frank Dahl Adam
- Rasmus Kabel Mollerup

**Data Center Norway**
Tore Heide Villund *(acting)*
- Leo Storm Omre *(team lead)*
- Kjell Arne Bjørnstad
- Ole Hjelmeland

Current description of GlobalConnect's 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.

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.

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 Global-Connect'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 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**

Operations is responsible for the day-to-day operations and monitoring of data centers. Moreover, Operations is responsible for Quality management, Service management in relation to customers and handling of planned work throughout the organisation.

Customer Care 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 (Customer Care), 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 Customer Care 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 Customer Care.

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 SOLUTIONS IN DENMARK AND 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 GlobalConnect'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 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
- 6 sites I Ejby
- 2 sites I Vallensbaek
- 1 site in Central Copenhagen
- 1 site in Copenhagen NV
- 1 site in Odense

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

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

High security is achieved by, among others, personal access control, 24-hour monitoring by Customer Care, 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

GlobalConnect 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.

GlobalConnect's 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 ASSESMENT

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's 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.

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.

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

GlobalConnect's Customer Care in Taastrup monitors all data centres, among others also video monitoring of entrances and gates to the areas. The Customer Care is staffed 24/7/365.

High security is achieved among others by personal access control, 24/7/365 staff monitoring from Customer Care 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.

Customer Care 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 Customer Care is responsible for sending warnings to customers. The warnings are also recorded in the Service Management System. Requests from customers to Customer Care 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 A/S as provider of all back-up of GlobalConnect's operating systems and Service Management System etc. GlobalConnect verifies that Frontsafe A/S 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.

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 CONTROLS IN RELATION TO DATA CENTER SOLUTIONS

In the period from 1 January to 31 December 2020 no material changes were made to GlobalConnect's controls in relation to Data Center solutions in Denmark and Germany.

# CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

### Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in GlobalConnect A/S' description of controls in relation to Data Center solutions and of the design and the operating effectiveness of these controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's test of the design and operating effectiveness of controls has included the control objectives and related control activities selected by GlobalConnect A/S, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 1 January to 31 December 2020.

### Tests performed

Tests of the design of technical and organisational security measures and other controls, the implementation and effectiveness hereof were performed by inquiry, inspection, observation and re-performance.

| Type | Description |
|---|---|
| Inquiry | Interviews of relevant personnel at GlobalConnect A/S have been performed for all significant control activities.<br><br>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.<br><br>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 assurance report for the period from 1 October 2019 to 30 September 2020 on technical and organisational security measures relating to operation of Cloud Backup services.

This subservice organisation's relevant control objectives and related controls are not included in Global-Connect A/S' description of controls related to Data Center solutions in Denmark and Germany. Accordingly, we have solely assessed the report and tested the controls at GlobalConnect A/S that monitor the operating effectiveness of the subservice organisation's controls.

**Result of tests**

The results of the tests performed of controls show whether the test has given rise to note exceptions.

An exception exists when:

- Controls have not been designed and implemented to achieve a control objective

- Controls relating to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

## 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**<br><br>▶   A risk assessment is performed annually which is ap-proved 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 GlobalConnect.<br><br>We have inspected GlobalConnect's information security policy, information security rules, and information security manual.<br><br>We have observed that the overall risk assessment is part of the work with the information security management system.<br><br>We have inspected GlobalConnect's risk assessment.<br><br>We have observed that the risk assessment applies to 2020. We were informed that threats and risks are assessed currently by the Quality and Security Committee.<br><br>We have observed that meetings are held regularly in Global-Connect's Quality and Security Committee, and we have in-spected selected minutes of meetings. We have observed that the purpose of the meetings is to ensure maintenance, raising and embedding of information security, including current as-sessment of threats and risks. | No exceptions noted. |

## 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**<br><br>▶ 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 GlobalConnect.<br><br>We have inspected GlobalConnect'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.<br><br>We have inspected GlobalConnect's terms of reference for the Quality and Security Committee set up, including procedures to ensure approval by management and communication within the organisation.<br><br>We have inspected the information security policy.<br><br>We have observed that the information security policy is communicated to employees and relevant external business partners and we have inspected relevant documentation. | No exceptions noted. |
| **Review of policies for information security**<br><br>▶ GlobalConnect has implemented an annual plan of controls which ensures periodical review of the information security policy.<br>▶ A written information security policy has been drawn up which is reassessed annually.<br>▶ The information security policy is updated and approved by Management. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's audit plan for review of information security policy, information security rules, and information security manual.<br><br>We have observed that a written information security policy has been drawn up which describes that the policy is reassessed annually.<br><br>We have observed that the information security policy was updated and approved by management in March 2020. | No exceptions noted. |

## 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 use of mobile equipment.*

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

## 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**<br><br>▶ A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee.<br>▶ Employment in GlobalConnect always requires that a "criminal record" can be presented.<br>▶ 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 GlobalConnect.<br><br>We have inspected GlobalConnect'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.<br><br>We have inspected the procedure for managing criminal records and observed that a criminal record must be presented in connection with any employment in GlobalConnect.<br><br>We have inspected an overview of new employees in 2020, and we have by random sampling selected and inspected documentation for new employees which follows GlobalConnect's procedures in this respect, including creation of employees in systems and presentation of criminal record.<br><br>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 exceptions noted. |
| **During employment**<br><br>▶ Employees at GlobalConnect are currently informed of information security matters and potential threats in relation to their tasks.<br>▶ Employees at GlobalConnect declare annually that they have read and accept the information security policy and the manual. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's Intranet. We have observed that the employees at GlobalConnect are kept updated on information security matters and any threats relating to their tasks. | No exceptions noted. |

| A.7: | Human resource security<br>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.<br><br>We inspected a list of personnel starting in 2020 and we have randomly selected and inspected documentation for new employees which complies with GlobalConnect's procedures in this respect, including confirmation by their signature that they have read and accepted the information security policy and manual. | |
| **Non-disclosure and confidentiality agreements**<br><br>▶ All employees working with confidential data – including personal data – have signed a non-disclosure agreement. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect'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.<br><br>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 exceptions noted. |

| A.7: | Human resource security<br>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 |
|---|---|---|
| **End or change of employment**<br><br>▶ After the end or change of the employment, accesses and rights are withdrawn or changed in accordance with the functional need in this respect.<br>▶ After the end of the employment, equipment received by the leaving employee is returned.<br>▶ After the end of the employment, HR ensures that the procedure for departure is complied with. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedure for employment and resignation of employees. We have inspected the form used in connection with resignation.<br><br>We have inspected randomly selected retired employees and observed that GlobalConnect's IT department prepares and sends a checklist of returned equipment to HR department.<br><br>We have randomly selected employees form the list of all resigned employees in 2020 and inspected whether the employees' access to the network was terminated and that the termination has been carried out on time.<br><br>We have inspected overview of employees who left in 2020, and we inspected resignation form for randomly selected employees, who have left. | No exceptions noted. |

| 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**<br><br>► Processes and procedures have been adopted to manage access and restrictions to systems and data based on business and functional requirements.<br>► All access and changes to access to systems and data follow the adopted processes and procedures. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedure for employment and resignation of employees, procedure for access control to physical locations and systems, procedure for user access for IT-systems and procedure for escorted access to GlobalConnect's data centres and other locations.<br><br>We have inspected documentation of the following sections of A.9 Access controls and observed that the processes and procedures approved are fulfilled. | No exceptions noted. |
| **User registration and deregistration**<br><br>► GlobalConnect has implemented and follows the process for creation and deregistration of users in systems. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedure for employment and resignation of employees. We have inspected onboarding and offboarding of employees.<br><br>We have inspected overview of new employees and employees who left in 2020, and we have randomly selected and inspected documentation for new and resigned employees, which complies with GlobalConnect's procedures in this respect.<br><br>We have observed that GlobalConnect carries out internal controls of users' access. | No exceptions noted. |

| 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**<br><br>▶ 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.<br>▶ 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 GlobalConnect.<br><br>We have inspected GlobalConnect's procedure for employment and resignation of employees.<br><br>We have inspected the creation of employees via JIRA and observed that the immediate manager chooses which areas the individual should have access to and which programs and rights the employee should be assigned.<br><br>We have inspected overview of newly employees in 2020, and we have randomly selected and inspected documentation for newly hired employees. We have observed that GlobalConnect's procedures are followed, including the allocation of access to systems and services.<br><br>We have randomly selected employees from a list of all employees resigned in 2020 and observed that the resigned employees' access was terminated on time. | No exceptions noted. |
| **Management of privileged access rights**<br><br>▶ GlobalConnect has implemented granting of administrative access to entities according to the functional need which is authorised.<br>▶ GlobalConnect has implemented logging of accesses with privileged accounts (administrative rights). | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedure for employment and resignation of employees. | No exceptions noted. |

| 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 have inspected overview of newly appointed employees in 2020, and we have randomly selected and inspected documentation for new employees, which complies with GlobalConnect's procedures in this respect, including granting of access to systems and services. We have observed that GlobalConnect has implemented a system for management, monitoring and logging of privileged accounts. | |
| **Management and use of passwords to users**<br><br>▶ GlobalConnect has implemented a process and rules for granting and management of passwords.<br><br>▶ GlobalConnect has implemented rules for establishment of passwords which must be followed by all employees and temporary consultants. | We have interviewed relevant personnel at GlobalConnect. We have inspected GlobalConnect's information security rules and information security manual for use of passwords, including procedure for user access to IT systems. We have inspected extracts of Password Policy and extracts of users in Active Directory. We have observed that the policies comply with GlobalConnect's password requirements, and that all employees and temporary consultants comply with GlobalConnect's password policy. | No exceptions noted. |

| 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**<br><br>▶ The established physical perimeter safety guarding is in agreement with the adopted security requirements. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedures for access control and escorted access to locations.<br><br>We have inspected the physical perimeter safeguarding relating to office buildings, selected data centres and selected repeater sites.<br><br>We observed, by random sampling, the handling of guest cards and we inspected the documentation of the selected samples. | No exceptions noted. |
| **Physical access control**<br><br>▶ Access controls have been established which guard against the probability of unauthorised physical access to, damage or interruption of GlobalConnect's premises and information – including ensuring that only authorised persons have access.<br>▶ Activities are recorded in the access control system Customer Care.<br>▶ Half-yearly review has been made of external access cards that have not been used within the last six months.<br>▶ Half-yearly review has been made of internal access cards that have not been used within the last six months.<br>▶ Test control of selected access points to ensure that the right persons have the right accesses. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedures for access control and escorted access to locations and procedure for access control in connection with employment and resignation of employees.<br><br>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 Customer Care. We have inspected documentation in this respect.<br><br>We have observed procedure for escorted access and inspected documentation in this respect in Service Management System by random sampling. | We found that GlobalConnect has not fully complied with the procedure for terminations of customers' access as deletion of 10 access cards for a single customer has not been carried out on time.<br><br>No further exceptions noted. |

| A.11: Physical and environmental security<br>      Secure areas and equipment | | |
|---|---|---|
| **Control objectives**<br>▶   *To prevent unauthorised physical access to and damage and interruption of the organisation's information and information processing facilities.*<br>▶   *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 randomly selected creations and termination of employees. We have inspected extract from the access control system and inspected key list of physical keys. We have observed the implemented access controls.<br><br>We have observed procedure for customers' and suppliers' access, including access as a guest or access to administrative areas.<br><br>We have inspected selected creations and termination of customers' and suppliers' access. We have inspected extracts from the access control systems. We have observed the established access controls.<br><br>We have inspected GlobalConnect'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**<br><br>▶   GlobalConnect complies with specified requirements for physical security for data center solutions including:<br>     • Building<br>     • Floors<br>     • Footprints<br>     • Climate<br>     • Power supply<br>     • Access<br>     • Alarm monitoring<br>     • Fire extinction<br>     • Cabling | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's information security policy, information security rules and information security manual.<br><br>We have inspected and observed the physical security measures for selected data centres. We observed that the physical security measures are based on specific risk assessments for the individual data centres.<br><br>We observed that the data centres 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 to data centers and the data centers are camera monitored. | No exceptions noted. |

## 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 doors to the data centres are fire-proof, and that the ceilings are coated with fire-resistant material.<br><br>We observed that automated fire control equipment is established in the data centres, that the floors are elevated and coated with antistatic flooring, and that humidity sensors are installed under the elevated floors.<br><br>We have observed that redundant cooling systems are installed in the data centres 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 Customer Care.<br><br>We have observed that power intake is attached to each data center, that the power and fiber are drawn under the elevated floor or placed in cable trays under the roof, and that emergency power supply is established. | |
| **Work in secure areas**<br><br>▶ GlobalConnect has established monitoring in data centres and suitable safeguarding of guidelines for activities and work in the areas. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected the GlobalConnect's information security policy, information security rules and information security manual.<br><br>We have inspected selected physical data centres and observed that, with respect to the data centres located in physical buildings, camera monitoring is installed, and that the data centres are monitored by Customer Care. We observed that the walking areas in the data centres are monitored 24 hours a day. | No exceptions noted. |

## 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 GlobalConnect's physical access control and protection measures against external and environmental threats. | |
| **Placing and protection of equipment**<br><br>▶ GlobalConnect has established suitable measures to prevent unauthorised access to customers' systems, data and information. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's procedures for access control and escorted access to locations and procedure for access control relating to new employments and resignation of employees.<br><br>We have inspected selected physical data centres 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.<br><br>We have inspected GlobalConnect's physical access control and protection measures against external and environmental threats. | No exceptions noted. |
| **Underlying supplies (supply reliability)**<br><br>▶ GlobalConnect has established and maintains equipment to ensure that the consequences of business interruption are mitigated.<br>▶ A check is made with respect established ventilation, cable trays, etc. according to a fixed template for inspection (maintenance report).<br>▶ GlobalConnect reviews maintenance reports. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected the procedure for planned work for the individual data centres in the Service Management System.<br><br>We have inspected documentation for randomly selected monthly maintenance reports from data centres. | No exceptions noted. |

## 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 and randomly inspected service and maintenance reports from these providers relating to the implemented security measures in data centres. | |
| **Maintenance of equipment**<br><br>▶ GlobalConnect performs monthly preventive inspection of data center facilities. The result of these inspections is documented in completed schedules.<br>▶ 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 at GlobalConnect.<br><br>We have inspected GlobalConnect's descriptions of procedures, internal controls and standard agreements.<br><br>We have inspected the procedure for planned work for the individual data centres in the Service Management System.<br><br>We have inspected documentation for randomly selected monthly reports from data centres.<br><br>We have inspected list of external providers. We have observed that GlobalConnect 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.<br><br>We have randomly inspected service and maintenance reports from providers relating to the implemented security measures in data centers. | No exceptions noted. |

## 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**<br><br>▶ GlobalConnect uses third-party provider (Frontsafe A/S) for all back-up of the operating systems and Service Management system<br>▶ Frontsafe A/S has documented its controls in an ISAE 3402 auditor's report which GlobalConnect reviews annually. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected Service Level Agreement from Frontsafe A/S relating to Cloud Backup services.<br><br>We observed that GlobalConnect has obtained independent auditor's ISAE 3402 assurance report for the period from 1 October 2019 to 30 September 2020 on technical and organisational security measures relating to the operation of Cloud Backup services.<br><br>We have inspected the above ISAE 3402 assurance report. | No exceptions noted. |
| **Change management**<br><br>▶ GlobalConnect has established a process for management of changes in data centers which is carried out according to defined routines for change management.<br>▶ Changes and management hereof are documented in Service Management System.<br>▶ Customers are warned before the change work is commenced to ensure least possible inconvenience for the customers. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected procedure for implementation and operation of data centres and procedure for change management, including instructions and check lists.<br><br>We observed that planned work is created and managed in the Service Management System, and that Customer Care 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. | No exceptions noted. |

## 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 extract from Service Management System of planned work for the period from 1 January to 31 December 2020.<br><br>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.<br><br>We have inspected documentation for randomly selected Change Management and Patch Management tasks in 2020. | |
| **Incident logging**<br><br>- Recording and handling of all relevant incidents have been established including attempts of unauthorised access to the systems.<br>- Network is monitored with software tools. Alarms have been set up which notify in case of network errors.<br>- All data centers are monitored by Customer Care, 24/7/365, and all incidents or alarm, from are examined immediately.<br>- 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 GlobalConnect.<br><br>We have inspected GlobalConnects procedures for monitoring of data center solutions, including procedures and guidelines for incident management, crisis management of critical errors and emergency preparedness.<br><br>We observed that monitoring in Customer Care is made in the systems and visually on screens, and that the implemented procedures and guidelines are followed, including recording of incidents.<br><br>We observed that incidents are recorded in Service Management System. We have inspected extracts from this system of all incidents happened and created in 2020 in the category Data Center solution. | No exceptions noted. |

## 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 randomly selected incidents in Service Management System with the priority critical and observed that response times are met. | |
| | We have inspected procedure for escalation of critical errors and observed that Customer Care follows the procedures. | |
| | We have inspected monthly reports from Customer Care. | |

## 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**<br><br>▶ All security incidents are managed in Service Management System and in accordance with established procedures. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnects 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.<br><br>We observed that incidents are recorded in Service Management System. We have inspected extracts from this system of all incidents happened and created in 2020.<br><br>We have inspected randomly selected incidents in Service Management System with the priority critical. We have inspected the procedure for escalation of critical errors and observed that Customer Care complies with the procedure. | No exceptions noted. |
| **Reporting of information security incidents**<br><br>▶ 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.<br>▶ Processes and procedures have been established to ensure recording and handling of security incidents by the right employee. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnects procedures and guidelines for incident management, crisis management of critical errors and emergency preparedness.<br><br>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.<br><br>We have inspected randomly selected incidents in Service Management System with the priority critical. We have observed that the implemented procedures are followed. | No exceptions noted. |

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

**Control objectives**

▶ *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**<br><br>▶ Contingency plans are prepared for Data centers to ensure business continuance in connection with security incidents, which are applicable for five years ahead.<br>▶ The contingency plans are updated periodically. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's overall risk assessment and the relating contingency plans and procedures. We have also inspected the procedure for Customer Care incident management and procedure for crisis management of critical errors and emergency preparedness.<br><br>We have observed that GlobalConnect 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 most recently were updated in 2019, and that they are applicable until 2023. | No exceptions noted. |
| **Verify, review and evaluate the information security continuity**<br><br>▶ 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.<br>▶ Contingency tests are documented by reports from testing. | We have interviewed relevant personnel at GlobalConnect.<br><br>We have inspected GlobalConnect's overall risk assessment and the relating contingency plans and procedures, including procedures for testing of contingency plans.<br><br>We have inspected GlobalConnect's plan for test of the contingency plans running from 2019 to 2023.<br><br>We have observed that GlobalConnect has performed the planned test of the emergency preparedness according to the plan. | No exceptions noted. |

| A.17: Information security aspects of business continuity management | | |
|---|---|---|
| **Information security contingency and redundancy** | | |
| **Control objectives** | | |
| ▶ *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** |
| | We have inspected the documentation for the tests in the form of prepared reports that refer to registrations in the Service Management System. We have observed that any comments or suggestions for improvement are followed up in GlobalConnect's Quality and Security Committee. | |

# SUPPLEMENTARY INFORMATION FROM GLOBALCONNECT A/S

| Action plan | | |
|---|---|---|
| Control activity | Result of test | Initiative |
| A.11: Physical access control | We found that GlobalConnect has not fully complied with the procedure for terminations of customers' access as deletion of 10 access cards for a single customer has not been carried out on time. | GlobalConnect has deleted the identified access cards immediately and initiated steps to ensure compliance with the procedures of managing customers' access. |