

JANUARY 2023

# GlobalConnect A/ S

ISAE 3402 TYPE 2 ASSURANCE REPORT

CVR 3326692

Independent auditor's report on the control environment related to the operation of Datacenter Solutions in Denmark and Germany.

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

[www.beierholm.dk](http://www.beierholm.dk)

# Structure of the Assurance Report

## Chapter 1:

Letter of Representation.

## Chapter 2:

Description of the control environment for the operation of Datacenter Solutions in Denmark and Germany.

## Chapter 3:

Independent auditor's assurance report on the description of controls, their design and operating effectiveness.

## Chapter 4:

Auditor's description of control objectives, security measures, test, and findings.

## CHAPTER 1:

# Letter of Representation

GlobalConnect A/S has prepared the following descriptions of controls in relation to Datacenter Solutions in Denmark and Germany.

The accompanying description has been prepared for the use of GlobalConnect A/S customers and their auditors, who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customer's financial statements.

GlobalConnect A/S hereby confirms that

- (A) The accompanying description, Chapter 2 gives a true and fair description of GlobalConnect A/S control environment in relation to operations of Datacenter Solutions in Denmark and Germany throughout the period 1 January 2022 - 31 December 2022. The criteria for this assertion are that the following description:
- (i) Presents how the services and relevant controls in relation to Datacenter 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 aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls relevant for the customers' Datacenter Solutions in Denmark and Germany.
  - (ii) Includes relevant information about changes in relation to Datacenter Solutions in Denmark and Germany throughout the period 1 January 2022 - 31 December 2022.
  - (iii) Does not omit or misrepresent information relevant for the scope of the controls described in relation to Datacenter Solutions in Denmark and Germany, taking into consideration that the description has been prepared to meet the common needs of a broad range of customers and their auditors, and may not, therefore, include every aspect of Datacenter Solutions in Denmark and Germany and control system that each individual customer may consider important in their own particular environment.
- (B) 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 1 January 2022 - 31 December 2022. The criteria for this assertion are that:
- (i) The risks threatening the fulfilment of the control objectives mentioned in the description were identified
  - (ii) The identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of the said control objectives, and
  - (iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competences and authority throughout the period 1 January 2022 - 31 December 2022.

Copenhagen, 31 January 2023

GlobalConnect A/S

Luke Davies

Head of Datacenters

# Description of the control environment for GlobalConnect A/ S

## GENERAL DESCRIPTION OF GLOBALCONNECT

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 to a number of national and international telecom companies providing services to private and public businesses, universities and educational institutions. Services are also provided to Danish businesses.

GlobalConnect A/S is part of Global Connect covering Denmark, Sweden, Norway, Germany and Finland and is owned by EQT infrastructure.

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 2 Assurance Report for the period from 1 January to 31 December 2022. The description of those controls, their design, and operating effectiveness are therefore not a part of this description.

## GENERAL DESCRIPTION OF THE GLOBALCONNECT'S ORGANISATION

Global Connects Executive Leadership Team covers the following roles

- Group CEO
- Group CFO, CTO, CIO, CMO, CHRO
- Country CEOs for Denmark/Germany, Sweden/Finland, and Norway
- Directors of B2C for Sweden and Norway
- Group Head of Digital Solutions

The following functions are central for the sales, delivery, and operations of Global Connect DKs (Denmark/Germany) services

- Sales organisation with offices in several locations in Denmark and Germany
- Product Management and Sales Support department
- Production, Delivery and Service Management
- Data Center organisation covering Global Connects Data Center operations, maintenance and building activities, located in Denmark and Germany
- Global Connect Outsourcing Services handling design and operation of cloud and outsourcing services
- Operations organisation with Customer Care, NOC, IT, and network operations
- Network and Infrastructure organisation covering development of same
- IT Development
- Security and Compliance
- Executive functions for Finance, HR, Legal and Administration

Description of main functions of GlobalConnect A/S' organisation.

### **Production, Delivery and Service Management**

Functions related to pre-operation phases are placed in Global Connect Denmark CEO organisation. This includes dedicated units for production, delivery, and service management.

### **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 GlobalConnect A/S' staff, however, in case of heavy workloads, subcontractors may be used for splicing of new fiber runs and planned changes of the network.

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

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

### **Operations**

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

Customer Care and Network Operation Center 1<sup>st</sup> and 2<sup>nd</sup> level support – Attended 24 hours a day, which monitors, operates, and maintains all platforms. In addition, Single Point of Contact for all operating projects.

Infrastructure Development/3rd level support - Responsible for expansion and maintenance of GlobalConnect A/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).

## **Security**

Security DK is responsible for defining, governing, and maintaining the baseline security level for the Global Connect DK. This is followed up through defined key security metrics and compliance measurements. For Global Connect DK Security DK governs, coordinates and steers security risk management.

Security DK is supported by a Group Security SOC that monitors and improves GlobalConnect's security posture while preventing, detecting, analyzing, and responding to cyber security incidents.

## **GENERAL DESCRIPTION OF DATA CENTER SOLUTION IN DENMARK AND NORTHERN GERMANY**

Data Center solutions are an important element of GlobalConnect A/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 A/S' network spine of fiber rings, which forms a big figure "eight" across Denmark, Sweden, and Northern Germany. The network's inherent redundancy ensures high transmission security and uptime for our customers' IT services and ensures that the communication direction can be reversed in case of cable breakdown or breakdown of transmission equipment.

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

GlobalConnect A/S' Customer Care – Operations & Maintenance Centre – in Copenhagen monitors closely Data Center solutions, among others by video monitoring of entrances and gates to the areas. 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 A/S 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 of which are identified in connection with the 24-hour monitoring.

### **General description of the overall control environment**

GlobalConnect A/S 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 A/S' ISMS is designed to follow the requirements of the international standard ISO/IEC ISO 27001. The relating control environment is managed by a dedicated compliance manager under the leadership of Security DK. Meetings are held regularly in GlobalConnect A/S' Security Boards, which are addressing strategic, business and operative levels.

### **Risk assessment**

Risk assessments are reviewed quarterly and updated once a year. The process is facilitated by the Strategic Security Board consisting of executive staff from relevant departments and chaired by Country CEO.

Risk assessments are based on the international standards ISO 31000 and ISO27005.

### **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 A/S 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 A/S 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 security board with participants from all relevant departments.

### Placing of responsibility for information security

All areas of responsibility for the information security are described in GlobalConnect A/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 A/S 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 pre-defined 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 is made available to all employees. All employees and consultants are part of regular security training.

### 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 A/S 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 and IT department.

### Closing down of access rights

GlobalConnect A/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 and IT department.

## **A.9 Access control**

GlobalConnect A/S 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 A/S has procedures for creation and closing of users which are placed in the HR and IT department.

### Extended rights

All rights are managed based on the employees' roles.

### Management of password

Granting of passwords is subject to the password policy which are set out in our Active Directory.

Furthermore, a password database is restricting users from utilizing common or simple passwords.

### **A.11 Physical and environment security**

GlobalConnect A/S' Customer Care in Copenhagen monitors all network and building monitoring systems, and Datacenter security monitors all door alarms amongst others also video monitoring of entrances and gates to the areas. The Customer Care and datacenter security is staffed 24/7/365.

High security is achieved among others by personal access control, 24/7/365 staff monitoring from Customer Care and Siteguard inclusive of, among others 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 Physical access control system.

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

### **A.12 Operations security**

GlobalConnect A/S 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.

GlobalConnect datacenters has a Technical board which serves to monitor and seize pan-Nordic GC-DC opportunities for technical growth and excellence

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.

A Threat & Vulnerability Risk Assessment (TVRA) is required for each site to identify the operational criticality of a site.

Deliveries to the datacenters are managed through the datacenter company portal via a ticket system.

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 Outsourcing Services provides backup for GlobalConnect A/S.

### **A.16 Information security incident management**

GlobalConnect A/S 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.

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

#### **A.17 business continuity management**

GlobalConnect A/S 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.

A risk register is in place and regularly updated. Risks are assessed and if necessary mitigated.

Contingency plans are prepared for Data Center which are updated at least once a year. The contingency plans are moreover regularly tested which ensures business continuance in case of 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 2022 no material changes were made to GlobalConnect A/S' services within Data Center solutions and relating controls.

## CHAPTER 3:

# Independent auditor's assurance report on the description of controls, their design and operating effectiveness

For the customers of GlobalConnect A/S' Datacenter Solutions in Denmark and Germany and their auditors.

### Scope

We have been engaged to report on GlobalConnect A/S' description in Chapter 2, which is a description of the control environment in connection with the operations of Datacenter Solutions in Denmark and Germany, throughout the period 1 January 2022 - 31 December 2022, as well as on the design and function of controls regarding the control objectives stated in the description.

We express our opinion with reasonable assurance.

### GlobalConnect A/ S' responsibility

GlobalConnect A/S is responsible for the preparation of the description and accompanying assertion in Chapter 2, including the completeness, accuracy, and method of presentation of the description and assertion; for providing the services covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

### Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality, and professional conduct.

We apply ISQC 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

### Auditor's responsibility

Our responsibility is to express an opinion, based on our procedures, on GlobalConnect A/S' description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and whether the controls in all material aspects are appropriately designed and operate 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 about the design and operating effectiveness of controls. The procedures selected depend on the judgement of the service organisation's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively.

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been 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 and described by GlobalConnect A/S in Chapter 2.

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

### **Limitations of controls at GlobalConnect A/ S**

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

### **Opinion**

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

- a) The description fairly presents control environment for the operation of Datacenter Solutions in Denmark and Germany, such as this control environment was designed and implemented throughout the period 1 January 2022 - 31 December 2022 in all material respects; and
- b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 January 2022 - 31 December 2022; and
- c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period 1 January 2022 - 31 December 2022.

### **Description of tests of controls**

The specific controls tested, and the nature, timing and findings of those tests are listed in Chapter 4.

### **Intended users and purpose**

This report and the description of the test of controls in Chapter 4 are solely intended for GlobalConnect A/S' customers and their auditors, who have sufficient understanding to consider them along with other information about controls operated by the customer themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Søborg, 31 January 2023

#### **Beierholm**

State Authorized Public Accountants  
CVR 32 89 54 68

Kim Larsen  
State-authorized Public Accountant

Poul Halkjær Nielsen  
It-auditor, CISSP, CISA CISM

## CHAPTER 4:

# Auditor's description of control objectives, security measures, test, and findings

We have structured our engagement in accordance with ISAE 3402 – Assurance Reports on Controls at a Service Organisation. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27001 and 27002.

With respect to the period, we have tested whether GlobalConnect A/S' has complied with the control objectives throughout the period 1 January 2022 - 31 December 2022.

Below the grey field are three columns:

- The first column tells the activities GlobalConnect A/S', according to its documentation, has put into practice in order to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

## The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to assess, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at GlobalConnect A/S'. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.

## Risk Assessment and Management

The risk assessment must be performed. The findings are to contribute to the identification and prioritisation of management interventions and precautionary measures necessary to address relevant risks.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
A risk assessment is performed annually which is approved by Management.	We have interviewed relevant management and staff at group and local level. We have inspected that an annual risk assessment is performed and approved by management. We have inspected that GlobalConnect's IS-standards prescribe that the assessment is updated minimum annually.	During our test, we did not identify any material deviations.



## CONTROL OBJECTIVE 5:

# Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies, and overall action plan. The information security policy will be maintained, taking the current risk assessment into consideration.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
Management sets out and approves policies for information security which after approval are published and communicated to staff.	<p>We have interviewed relevant management and staff at group and local level.</p> <p>We have inspected GlobalConnects latest IT-security policy.</p> <p>Through the audit we have inspected that it is maintained on a forthrunning basis.</p> <p>We have inspected that the policy is approved within the agreed governance structure for GlobalConnect in this subject area, and that the policy is available for all staff on the GlobalConnect intranet.</p>	During our test, we did not identify any material deviations.
GlobalConnect has implemented an ISMS to ensure periodical review of the information security policies.	<p>We have interviewed relevant management and staff at group and local level.</p> <p>We have inspected the current ISMS policy and seen that it requires a periodical review of the IS-policies.</p>	During our test, we did not identify any material deviations.
A written information security policy has been drawn up, which is reassessed and approved by management annually.	<p>We have interviewed relevant management and staff at local level.</p> <p>We have inspected the current information security policy and walked-through its maintenance with relevant staff. We have inspected that it is approved by management on a yearly basis.</p>	During our test, we did not identify any material deviations.

## CONTROL OBJECTIVE 6:

# Organisation of Information Security

Management of the IT security must be established in the company. Organisational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
The responsibility for the information security in GlobalConnect lies with the Management.	<p>We have interviewed relevant management and staff at group and local level.</p> <p>We have acquired relevant documentation for inspection that supports the control activity.</p> <p>We have inspected that it is stated in the Group documentation on information security that it is a management responsibility. This is also confirmed at the meetings where we have inquired into the matter, as well as through GlobalConnect management's participation in the company security fora.</p>	During our test, we did not identify any material deviations.
Management has appointed a three-layer model for steering activities related to security risks.	<p>We have interviewed relevant management and staff at group and local level.</p> <p>We have inspected the documents describing the three-layer model for steering activities related to security risks.</p> <p>We have inspected minutes of meetings that show activities related to security risks follow-up and decision making in security matters.</p>	During our test, we did not identify any material deviations.
GC has a group security unit with designated responsibility for local countries.	<p>We have interviewed relevant management and staff at group and local level.</p> <p>We have interviewed the security unit about its designated responsibilities and roles.</p> <p>We have inspected minutes of meetings that show activities related to information security risk follow-up and decision making.</p>	During our test, we did not identify any material deviations.

## CONTROL OBJECTIVE 7:

# Human Resource Security

It must be ensured that all new employees and contractors are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
A background check is made of all job candidates in accordance with business requirements and the function to be held by the employee.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the recruitment workflow. The presentation of an official police criminal record report is a default setting. Security clearance depends on the hiring managers specification.</p>	During our test, we did not identify any material deviations.
Employment at GlobalConnect requires that a criminal record can be shown.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the recruitment screenshots from the HR-workflow, and it clearly shows that the subject is part of the recruitment workflow routine.</p>	During our test, we did not identify any material deviations.
When a security clearance is required, this is obtained for the relevant employees in accordance with the relevant procedure.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the recruitment HR workflow and it clearly shows that the security clearance has its own workflow sub-routine.</p>	During our test, we did not identify any material deviations.
GlobalConnect carries out awareness training on a regular basis.	<p>We have interviewed relevant staff and management at GlobalConnect.</p> <p>We have inspected documentation that shows that awareness training is planned and occurs on a regular basis.</p>	During our test, we did not identify any material deviations.
Employees at GlobalConnect are required to read and accept the information security policy.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired into how it is required and ensured that employees sign off on this control as part of their signing their employment contract with GlobalConnect.</p> <p>We have inspected the information security policy.</p> <p>We have inspected documentation that it is an integral action in the employment contract process.</p> <p>We have inspected documentation that it is an integral action in the employment</p>	During our test, we did not identify any material deviations.

	process that employees are kept currently informed of the information security policy.	
All employees and consultants are required to sign a non-disclosure agreement.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired into how it is required and ensured that employees sign an NDA as part of their signing their employment contract with GlobalConnect.</p> <p>We have inspected documentation.</p>	During our test, we did not identify any material deviations.
After the end or change of the employment, accesses and rights are withdrawn or changed in accordance with the functional need in this respect.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the workflow.</p> <p>We have inspected documentation that IT Operations remove user rights and maintain the asset register.</p>	During our test, we did not identify any material deviations.
After the end of the employment, equipment received by the leaving employee is returned.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the workflow.</p> <p>We have inspected documentation that IT Operations remove user rights and maintain the asset register.</p>	During our test, we did not identify any material deviations.
GlobalConnect follows established procedures for on and off boarding.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the relevant procedures for on and off boarding and workflows.</p>	During our test, we did not identify any material deviations.

## CONTROL OBJECTIVE 9:

# Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be ensured, and unauthorised access must be prevented.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
Processes and procedures have been adopted to manage access and restrictions to systems.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected that HR feeds fundamental access requirements workflow based on a manager's approval.</p> <p>We have performed a walk-through of the process and the tasks at the meetings with the relevant functions.</p>	During our test, we did not identify any material deviations.
All access and changes to systems and data follow the adopted processes and procedures.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have performed a walk-through of the process and the tasks at the meetings with the relevant functions.</p> <p>We have inquired the relevant functions how and where Change is integral in relevant processes and procedures.</p> <p>We have inspected relevant samples.</p>	During our test, we did not identify any material deviations.
GlobalConnect has implemented and follows a process and procedure for creation and deregistration of users in systems.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have performed a walk-through of both the creation and the modification processes. We have inspected examples of use.</p>	During our test, we did not identify any material deviations.
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.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have performed a walk-through of both the creation and the modification processes. We have inspected examples of use.</p>	During our test, we did not identify any material deviations.
GlobalConnect has implemented a process and procedure for withdrawal or adjustment of access rights.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have performed a walk-through of both the creation and the modification processes. We have inspected examples of use.</p>	During our test, we did not identify any material deviations.

GlobalConnect has implemented granting of administrative access to entities according to the functional need which is authorised.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have performed a walk-through of both the creation and the modification processes. We have inspected examples of use.</p>	During our test, we did not identify any material deviations.
GlobalConnect has implemented logging of accesses with privileged accounts (administrative rights).	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the work routine ensuring that the three levels of users are assigned, and usage monitored.</p> <p>We have inspected the system for monitoring of privileged accounts and seen that monitoring is performed by another party in GlobalConnect.</p>	During our test, we did not identify any material deviations.
GlobalConnect has implemented a password policy for management of passwords.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>The security model and its implementation have been walked through.</p> <p>We have inspected documentation.</p>	During our test, we did not identify any material deviations.
GlobalConnect has implemented a password restriction database to avoid users using simple or commonly known passwords.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>The security model and its implementation has been walked through.</p> <p>We have inquired about the password restriction database and its implementation.</p> <p>We have inspected documentation.</p>	During our test, we did not identify any material deviations.

## CONTROL OBJECTIVE A.11: PHYSICAL AND ENVIRONMENTAL SECURITY

The control objective is to prevent unauthorized physical access to, and damage/disruption of the organization's information data processing facilities so as to avoid loss, damage, theft or compromise of assets and disruptions in the organization.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
GlobalConnect Data center technical board meet at least quarterly to discuss ideas, opportunities, and challenges concerning the datacenter solution.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to the assessment methodology for identifying and remediating ideas, opportunities, and challenges concerning datacenters.</p> <p>We have inspected minutes of meetings.</p>	During our test, we did not identify any material deviations.
Buildings are security zoned and protected by an Automated Access Control System (AACS) monitored by a 24/7, 365 days a year guard force.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to procedures and processes for the monitor.</p> <p>We have interviewed guard staff on-site regarding their monitoring tasks.</p>	During our test, we did not identify any material deviations.
Access to all areas containing critical information systems or their supporting documentation is strictly controlled and monitored.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to how it is ensured that all areas containing critical information systems, or their supporting documentation are controlled and monitored</p> <p>We have inquired if any incidents have occurred in the audit period and inspected their registration and resolution.</p>	During our test, we did not identify any material deviations.
Intrusion detection systems are in place combined with Visual Verification for the alarms. The alarms are monitored internally by security personnel at the Security Control Room 24/7, 365 days a year.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to procedures and processes for the monitor.</p> <p>We have inquired as to the setup, data security and functioning of the Visual Verification methodology applied.</p> <p>We have inquired if any incidents have occurred in the audit period and inspected their registration and resolution.</p>	During our test, we did not identify any material deviations.
All personnel, both permanent employees and visitors are given security identification	We have walked-through and inspected a sample of the datacenters to inspect that they comply with specified requirements for identification.	During our test, we did not identify any material deviations.

cards which are always visibly displayed.	We have interviewed and tested the site guard as to the consequences of not carrying security identification visibly.	
Once a year a risk assessment for each datacenter is being produced. The assessment covers specific physical threats that could impact operations on the site.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired into how the datacenter risk assessment aligns with the general information security policies and risks identified by the DK Security Group and Group Security.</p>	During our test, we did not identify any further material deviations.
A 'live' risk register is maintained to capture the day-to-day risks to each site.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to procedures and processes for maintenance of the live register and parameters qualifying a risk to be entered into the register.</p> <p>We have inspected the 'live register' on-site.</p>	During our test, we did not identify any material deviations.
A Threat & Environmental Vulnerability Risk Assessment is produced for every site.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to procedures and processes to produce the Threat &amp; Environmental Vulnerability Risk Assessment.</p> <p>We have inspected the current list of sites covered.</p> <p>We have taken out samples for inspection.</p>	During our test, we did not identify any material deviations.
The guardroom manages deliveries to the datacenters.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inquired as to procedures and processes for delivery.</p> <p>We have inspected a sample of designated delivery from the guard room and on-site areas.</p>	During our test, we did not identify any material deviations.
<p>GlobalConnect complies with specified requirements for physical security for repeater sites, including:</p> <ul style="list-style-type: none"> <li>• Buildings</li> <li>• Climate</li> <li>• Power supply</li> <li>• Access</li> </ul>	<p>We have walked-through and inspected a sample of the datacenters to inspect that they comply with specified requirements for physical security for repeater sites. This includes securing against:</p> <ul style="list-style-type: none"> <li>• fire</li> <li>• water damage</li> <li>• power interruption</li> <li>• loss of cooling</li> </ul>	During our test we did not identify any material deviations.



<ul style="list-style-type: none"> <li>• Alarm monitoring</li> <li>• Fire extinction</li> <li>• Cabling</li> </ul>	<ul style="list-style-type: none"> <li>• theft and vandalism</li> </ul> <p>We have:</p> <ul style="list-style-type: none"> <li>• Inspected the requirements</li> <li>• Inspected that there are fire extinguishing systems installed as well as cooling in the datacenters.</li> <li>• Reviewed and inspected maintenance documentation to confirm that UPS and diesel generators are maintained on a regular basis and tested.</li> <li>• During visits at the datacenters, we have inspected that maintenance and monitoring of UPS and diesel generators is performed.</li> <li>• Inspected for monitored climate control equipment in the datacenters.</li> <li>• Inspected that power and data cabling is protected.</li> <li>• Inspected that burglar alarms are mounted relevantly.</li> <li>• Inspected documentation of maintenance on a sampling basis.</li> </ul>	
<p>GlobalConnect complies with specified requirements for physical security for Datacenters, including:</p> <ul style="list-style-type: none"> <li>• Buildings</li> <li>• Climate</li> <li>• Power supply</li> <li>• Access</li> <li>• Alarm monitoring</li> <li>• Fire extinction</li> <li>• Cabling</li> </ul>	<p>We have walked-through and inspected that the datacenters GlobalConnect comply with specified requirements for physical security for Datacenters. This includes securing against:</p> <ul style="list-style-type: none"> <li>• fire</li> <li>• water damage</li> <li>• power interruption</li> <li>• loss of cooling</li> <li>• theft and vandalism</li> </ul> <p>We have:</p> <ul style="list-style-type: none"> <li>• Inspected the requirements</li> <li>• Inspected that there are fire extinguishing systems installed as well as cooling in the datacenters.</li> <li>• Reviewed and inspected maintenance documentation to confirm that UPS and diesel generators are maintained on a regular basis and tested.</li> <li>• During visits at the datacenters, we have inspected that maintenance and monitoring of UPS and diesel generators is performed.</li> </ul>	<p>During our test we did not identify any material deviations.</p>

	<ul style="list-style-type: none"> <li>Inspected for monitored climate control equipment in the datacenters.</li> <li>Inspected that power and data cabling is protected.</li> <li>Inspected that burglar alarms are mounted relevantly.</li> <li>Inspected documentation of maintenance on a sampling basis.</li> </ul>	
Half-yearly review has been made of external access cards that have not been used within the last six months.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have enquired into security zones or other ways access areas are defined.</p> <p>We have inspected control documentation for datacenters and office spaces.</p>	During our test we did not identify any material deviations.
Half-yearly review has been made of internal access cards that have not been used within the last six months.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have seen inspected documentation for datacenters and office spaces.</p>	During our test we did not identify any material deviations.
Weekly internal critical infrastructure test is performed by sites manager. The test reports are review by management.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have enquired into the definition of internal critical infrastructure and the type of tests performed as well as inspected documentation.</p>	During our test we did not identify any material deviations.
Before any work is done on sites, contractors need to fill out a risk and hazard assessment form which in turn needs to be approved by the site manager or operations manager.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have enquired into the use of the risk and hazard assessment form as well as the parameters for approval or denial.</p> <p>We have inspected documentation for the use of the risk and hazard assessment form.</p>	During our test we did not identify any material deviations.
Contractors needs to agree to and sign GlobalConnects data-center rules, which is part of the risk and analysis form, before any work is carried out.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected GlobalConnects data-center rules.</p> <p>We have enquired into the de facto enforcement of the rules as well as asked if there are any supplementary instructions given when handing out the access card.</p>	In the course of testing, we have found that the local IS-policy used for this control does not fully effectively address all relevant issues it should cover.

		During our test we did not identify other material deviations.
GlobalConnect reviews external maintenance reports once a year.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have enquired into the processing and documentation of said preview process.</p>	During our test we did not identify any material deviations.
GlobalConnect performs preventive inspection of repeater sites. The result of these inspections is documented in completed schedules.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected control documentation.</p>	During our test we did not identify any material deviations.
GlobalConnect has established periodical maintenance of cooling systems and generators at repeater sites of external organizations.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have on-site inspected a sample of repeatersites and datacenters.</p> <p>We have inspected control documentation for inspection.</p>	During our test we did not identify any material deviations.

## Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
GlobalConnect Outsourcing Services provides backup for Datacenter Management Services if requested	We have interviewed relevant staff at GlobalConnect.  We have inspected documentation for the control.	During our test, we did not identify any material deviations.
GlobalConnect has established a process for management of changes in data centers which is carried out according to defined routines for change management.	We have interviewed relevant staff at GlobalConnect.  We inquired into how changes follow the GlobalConnect change process.	During our test, we did not identify any material deviations.
Changes and management hereof are documented in Service Management System.	We have interviewed relevant staff at GlobalConnect.  We have walked through the change process at GlobalConnect for standard, changes, major changes, and e-changes including the standing CAB.  We have inspected examples of changes in the service management system.	During our test, we did not identify any material deviations.
Customers are warned according to a defined time schedule before the change to ensure least possible inconvenience for the customers.	We have interviewed relevant staff at GlobalConnect.  We have inquired about the process.  We have inspected documentation.	During our test, we did not identify any material deviations.
Recording and handling of all relevant incidents has been established.	We have interviewed relevant staff at GlobalConnect.  We have inspected the surveillance monitors and interviewed staff in the Customer Care.	During our test, we did not identify any material deviations.
Network is monitored with software tools. Alarms have been set up which notify in case of network errors.	We have interviewed relevant staff at GlobalConnect.  We have inspected the surveillance monitors and interviewed staff in the Customer Care.	During our test, we did not identify any material deviations.

<p>All data centers are monitored by Customer Care and Siteguard 24/7/365 and every incident or alarm is examined immediately.</p>	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the surveillance monitors and interviewed staff in the Customer Care and Siteguard.</p> <p>We have enquired into procedures and processes that govern the monitoring.</p>	<p>During our test, we did not identify any material deviations.</p>
<p>An incident report is opened in Service Management System on all errors with a reference number, which is used throughout the following error handling process.</p>	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the surveillance monitors and interviewed staff in the Customer Care.</p> <p>We have inspected a sample of incident reports opened to inspect if the reference number is used continually from opening to closure of an incident.</p>	<p>During our test, we did not identify any material deviations.</p>

## Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
All security incidents are managed in Service Management-System, and in accordance with established procedures.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have inspected the surveillance monitors and interviewed staff in the Customer Care.</p>	During our test, we did not identify any material deviations.
Processes and procedures have been established to ensure recording and handling of security incidents by the right employee.	<p>We have interviewed relevant staff at GlobalConnect.</p> <p>We have walked through the process and seen documentation.</p> <p>We have inspected the surveillance monitors and interviewed staff in the Customer Care.</p>	During our test, we did not identify any material deviations.

## Information Security Aspects of Business Continuity Management

Business continuity management is to counteract interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
Continuity plans are prepared for critical infrastructure to ensure business continuance.	We have interviewed relevant staff at GlobalConnect.  We have inspected the continuity plans and enquired into the definition of critical infrastructure.	During our test, we did not identify any material deviations.
The Continuity plans are updated periodically.	We have interviewed relevant staff at GlobalConnect.  We have inspected that the continuity plans are periodically updated.	During our test, we did not identify any material deviations.
GlobalConnect has established periodical testing of Continuity plans for the purpose of ensuring that the contingency plans are up-to-date and effective in critical situations.	We have interviewed relevant staff at GlobalConnect.  We have enquired as to how the tests ensure that the continuity plans are effective.  We have inspected that the continuity plans are periodically tested.	During our test, we did not identify any material deviations.
Continuity tests are documented by reports from testing.	We have inspected that the continuity plan tests are documented in reports.	During our test, we did not identify any material deviations.

# PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

“Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument.”

## Kim Larsen

State Authorized Public Accountant

På vegne af: Beierholm

Serienummer: CVR:32895468-RID:34629841

IP: 212.98.xxx.xxx

2023-01-31 12:58:27 UTC

NEM ID 

## Poul Halkjær Nielsen


It-auditor

På vegne af: Beierholm

Serienummer: CVR:32895468-RID:50750152

IP: 212.98.xxx.xxx

2023-01-31 13:02:22 UTC

NEM ID 

## Luke Mercer Davies

Head of Datacenters

Serienummer: 2a53e90e-48d3-42ac-936a-1ba530f13088

IP: 217.74.xxx.xxx

2023-02-01 10:17:58 UTC

Mit  

Penneo dokumentnøgle: Z3YJT-8SGOA-UMJ05-11EHA-61DCB-NTHXE

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

### Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service** <penneo@penneo.com>. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske s igneringsbeviser i ndlejret i dokumentet ved at anvende Penneos validator på følgende websted: <https://penneo.com/validator>