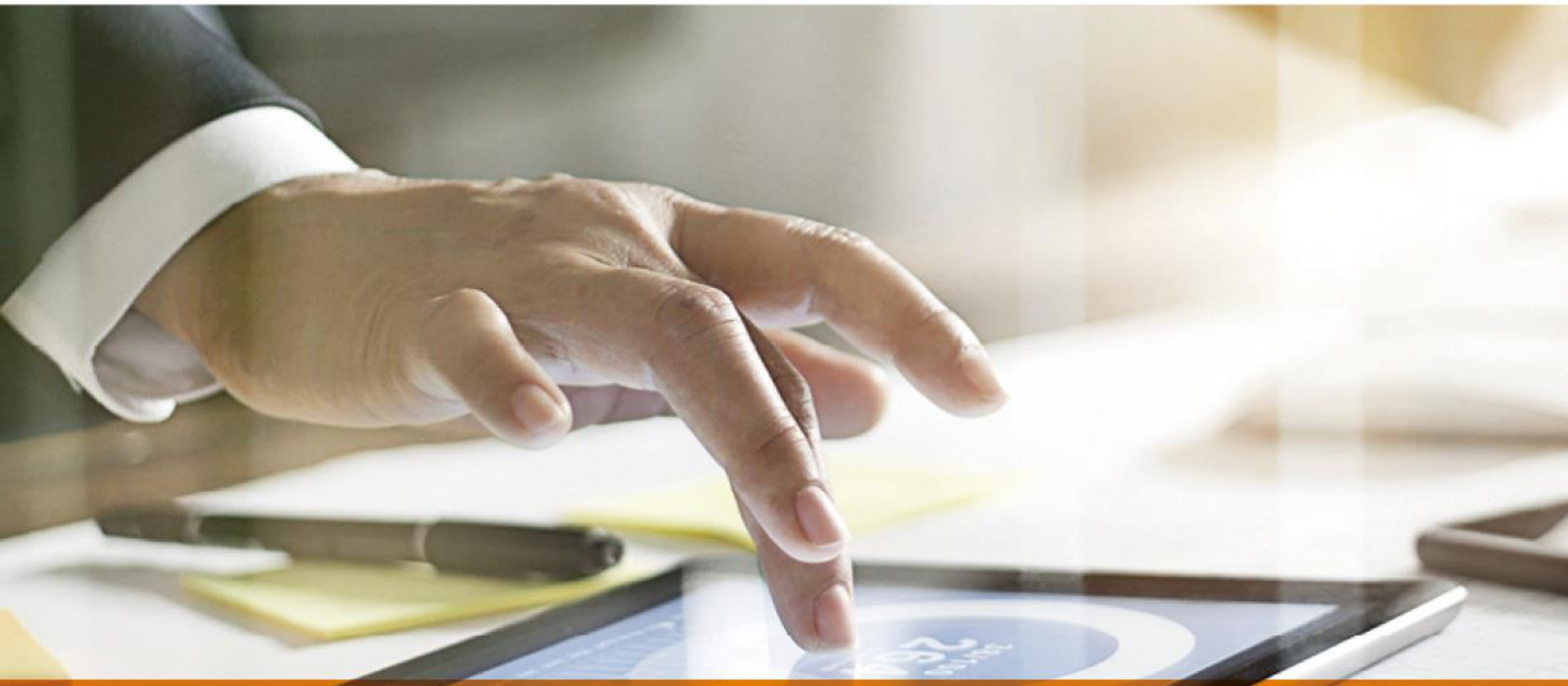
BEIERHOLM
VI SKABER BALANCE



JANUARY 2022

GlobalConnect A/S

ISAE 3402 TYPE 2 ASSURANCE REPORT

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

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, tests and findings.

CHAPTER 1:

Letter of Representation

GlobalConnect A/S har 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 2021 - 31 December 2021. 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 2021 - 31 December 2021.

(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 2021 - 31 December 2021. 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 2021 - 31 December 2021.

Copenhagen, 27. January 2022

GlobalConnect A/S

Louise Hahn

Country CEO DK & Germany

CHAPTER 2:

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 2021. The description of those controls, their design, and operating effectives, and 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 places 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 1st 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.

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 systems 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 down 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 a number of rules which are set out in our Active Directory.

A.11 Physical and environment security

GlobalConnect A/S' Customer Care in Copenhagen 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 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.

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 A/S uses Frontsafe A/S as provider of all back-ups of GlobalConnect A/S' operating systems and Service Management System etc. GlobalConnect A/S 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 A/S' requirements for back-up.

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 2021 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 2021 - 31 December 2021, 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 2021 - 31 December 2021 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 2021 - 31 December 2021; 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 2021 - 31 December 2021.

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, 28. January 2022

Beierholm
State Authorized Public Accountants
CVR 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Poul Halkjær Nielsen
Advisor, CISA

CHAPTER 4:

Auditor's description of control objectives, security measures, tests 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 2021 - 31 December 2021.

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.

CONTROL OBJECTIVE - INTRODUCTION:

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. The risk assessment is a part of the work with GlobalConnect's information security management system (ISMS).	We have interviewed relevant staff and acquired documentation. We have checked that GlobalConnect forth running works with risk assessments as part of their business area and development We have checked that risk is an integral part of the business' daily work routines.	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 and relevant external parties.	We have inspected GlobalConnects latest IT-security policy. Through the audit we have checked that it is maintained on a forth running basis We have checked 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	During our test, we did not identify any material deviations.
GlobalConnect has prepared and implemented a procedure to ensure periodical review of the information security policy.	We have interviewed relevant staff and acquired documentation. The documentation supports the control activities. At group level a mandatory requirement, split into quarterly activities has been formulated, stating that maintenance must occur at least on a yearly basis.	During our test, we did not identify any material deviations.
A written information security policy has been drawn up, which is reassessed annually.	We have interviewed relevant staff and acquired relevant documentation. At group level a mandatory requirement, split into quarterly activities has been formulated, stating that maintenance must occur at least on a yearly basis.	During our test, we did not identify any material deviations.
The information security policy is approved by management.	We have inspected GlobalConnects latest IT-security policy. We have checked that the policy is approved within the agreed governance structure for GlobalConnect in this subject area.	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.	We have interviewed relevant staff and management. We have acquired relevant documentation that supports the control activity. It is clearly stated in the Group documentation on information security that it is a management responsibility. This is also confirmed at the meetings as well as through GlobalConnect management's participation in the company security fora.	During our test, we did not identify any material deviations.
Management has appointed a cross-organisational Quality and Security Committee which considers activities relating to safeguarding of the information security.	We have interviewed relevant staff and management. We have been informed that the Quality & Security Committee has stopped and a new board has been formed, and which is headed by management. We have inspected minutes of meetings that show an active follow-up and decision making in information security matters.	During our test, we did not identify any material deviations.
Management has designated a Quality and Security Manager who has the overall responsibility for handling the information security.	We have interviewed relevant staff and management. Interview with the DK management and the Group CISO have confirmed the roles existence and position.	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.	We have interviewed relevant staff at GlobalConnect. We have inspected the recruitment workflow. The presentation of an official police criminal record report default setting. Security clearence depends on the hiring managers specification.	During our test, we did not identify any material deviations.
Employment at GlobalConnect requires always that an unblemished criminal record can be shown.	We have interviewed relevant staff at GlobalConnect. We have inspected the recruitment screenshots from one HR workflow and it clearly shows that the subject is part of the recruitment workflow routine.	During our test, we did not identify any material deviations.
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 staff at GlobalConnect. We have inspected the recruitment HR workflow and it clearly shows that the security clearance has its own workflow sub-routine.	During our test, we did not identify any material deviations.
Employees at GlobalConnect are currently informed of information security matters and potential threats in relation to their tasks.	We have interviewed relevant staff at GlobalConnect. We have inspected awareness campaign documentation, NDA's and seen documentation of the subject being part of staff meetings as well as in reporting to management.	During our test, we did not identify any material deviations.
Employees at GlobalConnect declare at the start of employment that they have read and accept the information security policy and the manual.	We have interviewed relevant staff at GlobalConnect. We have been informed that it is required that employees sign off on this control as part of their signing their employment contract with GlobalConnect.	During our test, we did not identify any material deviations.
All employees working with confidential data – including personal data – have signed a non-disclosure agreement.	We have interviewed relevant staff at GlobalConnect.	During our test, we did not identify any material deviations.

	We have been informed that it is required that employees sign an NDA as part of their signing their employment contract with GlobalConnect.	
After the end or change of the employment, accesses and rights are withdrawn or changed in accordance with the functional need in this respect.	We have interviewed relevant staff at GlobalConnect. We have inspected the workflow. IT Operations remove users rights and maintain the asset register.	During our test, we did not identify any material deviations.
After the end of the employment, equipment received by the leaving employee is returned.	We have interviewed relevant staff at GlobalConnect. We have inspected the workflow. IT Operations remove users rights and maintain the asset register.	During our test, we did not identify any material deviations.
After the end of the employment, HR ensures that the procedure for resignation is complied with.	We have interviewed relevant staff at GlobalConnect. We have inspected the workflow. IT Operations remove users rights and maintain the asset register.	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 and data based on business and functional requirements.	We have interviewed relevant staff at GlobalConnect. HR feeds the fundamental access requirements workflow based on a manager's approval. We have performed a walk-through of the process and the tasks at the meetings with the relevant functions.	During our test, we did not identify any material deviations.
All access and changes to access to systems and data follow the adopted processes and procedures.	We have interviewed relevant staff at GlobalConnect. There exists several procedures and processes.	During our test, we did not identify any material deviations.
GlobalConnect has implemented and follows the process for creation and deregistration of users in systems.	We have interviewed relevant staff at GlobalConnect. There exist several procedures in the procedure platform. We have performed a walk-through of both the creation and the modification processes. We have observed examples of use.	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.	We have interviewed relevant staff at GlobalConnect. There exist several procedures in the procedure platform. We have performed a walk-through of both the creation and the modification processes. We have observed examples of use.	During our test, we did not identify any material deviations.
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 staff at GlobalConnect. There exist several procedures in the procedure platform. We have performed a walk-through of both the creation and the modification processes. We have observed examples of use.	During our test, we did not identify any material deviations.
GlobalConnect has implemented granting of administrative access to entities according	We have interviewed relevant staff at GlobalConnect.	During our test, we did not identify any material deviations.

to the functional need which is authorised.	There exist several procedures in the procedure platform. We have performed a walk-through of both the creation and the modification processes. We have observed examples of use.	
GlobalConnect has implemented logging of accesses with privileged accounts (administrative rights).	We have interviewed relevant staff at GlobalConnect. There exists a work routine ensuring that the three levels of users are assigned and usage monitored. We have inspected the system for monitoring of privileged accounts and seen that monitoring is performed by another party in GlobalConnect.	During our test, we did not identify any material deviations.
GlobalConnect has implemented a process and rules for granting and management of passwords.	We have interviewed relevant staff at GlobalConnect. The security model and its implementation have been walked through.	During our test, we did not identify any material deviations.
GlobalConnect has implemented rules for establishment of passwords which must be followed by all employees and temporary consultants.	We have interviewed relevant staff at GlobalConnect. The security model and its implementation have been walked through.	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
The established physical perimeter safety guarding is in agreement with the adopted security requirements.	We have walked-through and inspected that the datacenters live up to the requirements set by management. This includes securing against: • fire • water damage • power interruption • loss of cooling • theft and vandalism We have: • checked that there are fire extinguishing systems installed as well as cooling in the datacenters. • Reviewed and checked maintenance documentation to confirm that UPS and diesel generators are maintained on a regular basis and tested. • During visits at the datacenters, we have observed that maintenance and monitoring of UPS and diesel generators is performed. • Checked for monitored climate control equipment in the datacenters. • Seen that power and data cabling is protected. • Seen that burglar alarms are mounted relevantly. • Checked documentation of maintenance on a sampling basis.	During our test we did not identify any material deviations.
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.	We have interviewed relevant staff at GlobalConnect. We have observed access control both in the offices, in datacenters and at repeatersites. GlobalConnect have an approval procedure for being assigned access rights in the access control system.	During our test we did not identify any material deviations.

Activities are recorded in the access control system OMC.	We have interviewed relevant staff at GlobalConnect. We have performed on-site inspection in the Customer Care. We have observed access control both in the offices, in datacenters and at repeatersites.	During our test we did not identify any material deviations.
Half-yearly review has been made of external access cards that have not been used within the last six months.	We have interviewed relevant staff at GlobalConnect. We have seen control documentation.	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.	We have interviewed relevant staff at GlobalConnect. We have seen control documentation.	During our test we did not identify any material deviations.
Test control of selected access points to ensure that the right persons have the right accesses.	We have interviewed relevant staff at GlobalConnect. Management authorizes access rights through a workflow procedure. We have inspected documentation.	During our test we did not identify any material deviations.
GlobalConnect complies with specified requirements for physical security for repeater sites, including: • Buildings • Climate • Power supply • Access • Alarm monitoring • Fire extinction • Cabling	We have on-site inspected a sample of repeatersites and datacenters in DK and DE. At all sites we have found adequate protection against external and environmental threats.	During our test we did not identify any material deviations.
GlobalConnect has established suitable measures to prevent unauthorized access to customers' systems, data and information.	We have on-site inspected a sample of repeatersites and datacenters in DK and DE. At all sites we have found adequate protection against unauthorized access.	During our test we did not identify any material deviations.

GlobalConnect has established and maintains equipment to ensure that the consequences of business interruption are mitigated.	We have on-site inspected a sample of repeatersites and datacenters in DK and DE and found aptly maintained equipment. We have received copies of maintenance records.	During our test we did not identify any material deviations.
A check is made with respect established ventilation, cable trays, etc. according to a fixed template for inspection (maintenance report) of repeater sites.	We have interviewed relevant staff at GlobalConnect. We have seen control documentation.	During our test we did not identify any material deviations.
GlobalConnect reviews maintenance reports.	We have interviewed relevant staff at GlobalConnect. We have been informed that the maintenance reports are reviewed.	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.	We have interviewed relevant staff at GlobalConnect. We have seen control documentation.	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.	We have interviewed relevant staff at GlobalConnect. We have on-site inspected a sample of repeatersites and datacenters in DK and DE. We have received control documentation and observed maintenance being performed at several sites.	During our test we did not identify any material deviations.

CONTROL OBJECTIVE 12:

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 uses third-party provider (Frontsafe A/S) for all back-up of the operating systems.	We have interviewed relevant staff at GlobalConnect. We have seen documentation for the control.	During our test, we did not identify any material deviations.
Frontsafe A/S has documented its controls in an ISAE 3402 auditor's report which GlobalConnect reviews annually.	We have interviewed relevant staff at GlobalConnect. We have seen documentation for the control.	During our test, we did not identify any material deviations.
GlobalConnect has established a process for management of changes datacenters which is carried out according to defined routines for change management.	We have interviewed relevant staff at GlobalConnect. We are informed that 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 observed 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 been informed about the process.	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.	During our test, we did not identify any material deviations.

	We have inspected the surveillance monitors and interviewed staff in the Customer Care.	
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.
All datacenters are monitored by Customer Care 24/7/365 and every incident or alarm is examined immediately.	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.
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 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.

CONTROL OBJECTIVE 16:

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.	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.
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.	We have interviewed relevant staff at GlobalConnect. We have walked through the process and seen documentation. We have inspected the surveillance monitors and interviewed staff in the Customer Care.	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.	We have interviewed relevant staff at GlobalConnect. We have walked through the process and seen documentation. The process has been explained in its ITIL context.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 17:

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
Contingency plans are prepared for Operations (Customer Care), to ensure business continuance in connection with security incidents, which are applicable for five years ahead.	We have interviewed relevant staff at GlobalConnect. Contingency plans consist of the respective internal functions major incident plans. These are mandated updated yearly by Group directives.	During our test, we did not identify any material deviations.
The contingency plans are updated periodically.	We have interviewed relevant staff at GlobalConnect. Contingency plans consist of the respective internal functions major incident plans. These are mandated updated yearly by Group directives. They are currently being assembled in to one plan.	During our test, we did not identify any material deviations.
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.	We have interviewed relevant staff at GlobalConnect. Tests are performed 1-2 times a year.	During our test, we did not identify any material deviations.
Contingency tests are documented by reports from testing.	We have interviewed relevant staff at GlobalConnect. Tests are performed 1-2 times a year. We have inspected test documentation.	During our test, we did not identify any material deviations.