BEIERHOLM
VI SKABER BALANCE

JANUARY 2024

GlobalConnect A/S

ISAE 3402 TYPE 2 ASSURANCE REPORT

Independent auditor's report on the control environment related to the operation of GlobalConnect Outsourcing Services.

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

www.beierholm.dk

Structure of the Assurance Report

Chapter 1:
Letter of Representation.

Chapter 2:
Description of the control environment for the operation of GlobalConnect Outsourcing Services.

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 has prepared the following descriptions of controls in relation to GlobalConnect Outsourcing Services.

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 utilizes a service sub-organization for data backup. The service sub-organization's control objectives and controls are not part of the following description (partial method).

The Data Center department at GlobalConnect A/S is service sub-organisation in relation to the physical security in the data centers from which GlobalConnect Outsourcing Services are operated. The description does not include control objectives and controls managed by the Data Center department and thus includes solely control objectives and controls relating to processes and procedures managed by GlobalConnect Outsourcing Services (partial method).

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 GlobalConnect Outsourcing Services throughout the period 1 January 2023 - 31 December 2023. The criteria for this assertion are that the following description:

(i) Presents how the services and relevant controls in relation to GlobalConnect Outsourcing Services 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.
- The controls that we, referring to the design of our services, have assumed were implemented by the customer and, if necessary, to achieve the control objectives stated in the description, were identified in the description along with the specific control objectives that we cannot achieve.
- Other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls relevant for the services provided.

(ii) Includes relevant information about changes in relation to GlobalConnect Outsourcing Services throughout the period 1. January 2023 - 31 December 2023.

(iii) Does not omit or misrepresent information relevant for the scope of the controls described in relation to GlobalConnect Outsourcing Services, 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 GlobalConnect Outsourcing Services 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 2023 - 31 December 2023. 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 2023 - 31 December 2023.

(C) The enclosed description and the criteria for attaining the control objectives and controls, chapter 2, have been developed on the basis of compliance with GlobalConnect A/S' standard agreement. The criteria forming the basis are:

(i) Service Level Agreement version 1.4
(ii) Dataprocessing agreement DK version 1.2

Copenhagen, 30 January 2024

GlobalConnect A/S

Monika Juul Henriksen

Head of B2B DK and CEO DK

CHAPTER 2:

Description of the control environment for GlobalConnect A/S

GENERAL DESCRIPTION OF GLOBALCONNECT A/S

GlobalConnect A/S (GlobalConnect), part of Nordic Connectivity AB, is a provider of Dark Fiber solutions, Transmission solutions, Outsourcing Services, including Cloud services, and Data Center solutions in Denmark to several national and international private and public companies.

This description is prepared with the purpose of reporting on the general controls which GlobalConnect Outsourcing Services (GCOS) applies to support and safeguard IT/Outsourcing/Cloud Services to its customers. The description focuses on business-related control objectives and processes implemented.

The Data Center department at GlobalConnect A/S is service sub-organisation in relation to the physical security in the data centers from which GCOS is operated. This description does not include control objectives and controls managed by the Data Center department.

DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES

GlobalConnect outsourcing services (GCOS) has since 2001 specialised in providing IT outsourcing and IT services to a wide range of public and private businesses in the Danish market. As a medium-sized provider, GCOS has been able to maintain a unique focus on supporting our customers' ability to operate an effective business in a public or private context. And what is more, this is without negative effects on the very fundamental IT capacities: stability, cost efficiency, scalability and, not least, operating reliability.

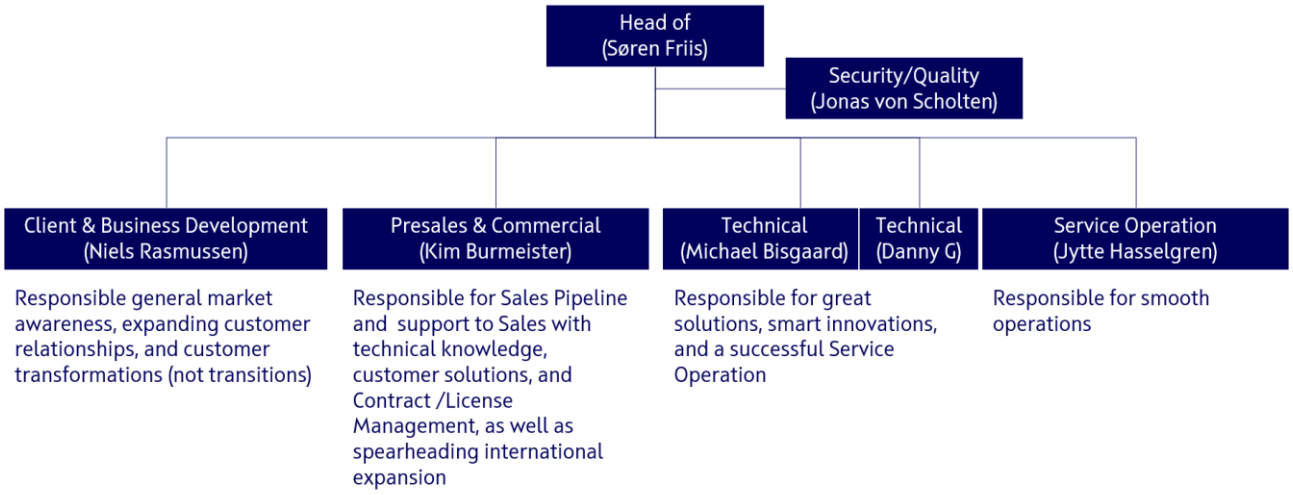
GCOS has throughout the years had a unique focus on customer satisfaction by means of quality assurance.

GCOS has implemented a quality management system based on the requirements in ISO 9001:2015, which aims at continuously enhancement of the quality of all deliveries. This means that all parts of the delivery process are subject to quality assurance; from appointment of suppliers, over internal policies for i.e., staff, compliance with all relevant public authority and regulatory requirements, to the quite central ITIL-based operating processes.

As a specialised outsourcing/cloud-partner, GCOS' principal duty is to provide stable and secure 24/7 operations and maintenance practice, this means that GCOS delivers at the agreed service levels (SLAs and KPIs), and that the business relationship with GCOS contributes actively to value creation and technological development for GCOS' customers. And GCOS' customers will have access to" critical mass" in the form of expert technological operations, expert knowledge, processes, and security. GCOS' customers may thus focus their resources on their core business.

GENERAL DESCRIPTION OF GLOBALCONNECT OUTSOURCING SERVICES' ORGANISATION

GCOS has several high tier partnerships with several significant technology vendors. Some of these are Microsoft CSP Gold Partner, VMware VCPP (VMware Cloud Provider Program) and Dell Platinum Partnership. GCOS' staff have relevant certifications within ITIL and the technologies provided to GCOS customers. Following organisational chart shows GCOS' formal organisation of functions:



RISK MANAGEMENT OF GLOBALCONNECT OUTSOURCING SERVICES

A risk assessment(s) are carried out periodically, or at least once every year, and input for this assessment is obtained from all levels in the organisation and by regulatory and public authority requirements. The process is facilitated by a quality and security committee consisting of executive staff from relevant departments. The assessment is presented to the company's senior management for approval. A contingency plan is also prepared annually which corresponds with the risk level of the organisation..

Moreover, it is only natural that risks are assessed and managed at tactical and operational level. In practice, risk assessments are an explicit element of several of our ITIL-based operating processes and we record potential security-related incidents caused by both external and internal conditions in our Servicedesk system for the purpose of a subsequent analysis.

Risk assessments are based on the implementation guidelines in the international standard ISO 27005.

The likelihood and consequence of the threats are (re)assessed based on the information existing at the time of the assessment. This reflects, in combination, the threat level. When the threat level has been determined, it is assessed to which extent the security environment considers the relevant threat level and, from where, it can be assessed, what the level of residual risk is.

GCOS has a formal process for management of risks which result in specific action plans. The action plans are allocated and addressed according to the adopted risk treatment procedure.
The day-to-day Management of GlobalConnect decides, based on the risk assessment, whether an identified risk can be accepted, is to be mitigated or whether insurance is required based on selected risks.

This report only includes controls and control objectives for processes and controls that are managed by GCOS and, thus, it does not include controls or control objectives that are managed by sub-organizations or parts of shared processes, regarding those parts that are managed outside GCOS.

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR CONTROL IMPLEMENTATION

GCOS' information security is defined based on the objective to provide dedicated IT outsourcing and high-quality infrastructure solutions, including stability and security.

The determination of criteria and scope of control implementation at GCOS is based on the ISO 27001:2013 - Annex A, referenced in ISO 27002, Code of practice for information security controls. The following control areas in ISO 27001 – Annex A has been assessed:

- A.5. Information security policy
- A.6. Organisation of information security
- A.7. Human resource security
- A.8. Asset management
- A.9. Access management
- A.10. Cryptography
- A.11. Physical and environmental security
- A.12. Operations security
- A.13. Communications security
- A.14. Acquisition, development, and maintenance of systems
- A.15. Supplier relationships
- A.16. Information security incident management
- A.17. Information security aspects of contingency, disaster recovery and restore management
- A.18. Compliance

Implemented control environment
The implemented controls are based on the management systems leveraged by GCOS to provide services to customers and include control areas and control activities within operation and hosting. The areas above are described in detail in the following in separate paragraphs, and the described control objectives and controls for those areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

A.5 Information security policy
GlobalConnect has established 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 periodically in relation to information security policies and the relevant manuals. In addition, a more detailed security policy is established for GCOS, with easy access for all staff, and with annual reminders on the objectives of the policy and how to access more details.
A.6 Organization of information security
GCOS 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 IT security in the organization. The formal responsibility, including approval of the information security policy, is ultimately that of the head of the organisation, however the responsibility can be delegated to relevant management representatives of any business unit.

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

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

Mobile data processing and communication

GCOS' policies and rules set out guidelines for use of mobile equipment outside the company. Employees can access the network from the outside exclusively via VPN or through use of secured jumphosts.

Access from home workplace is secured via encrypted VPN connection or a remote workplace environment, which requires validation via Active Directory utilizing multifactor authentication.

Authentication of users on external connections
All access to our network, including external users, is authorised by our formal Access Management procedure.

A.7 Human resource security
GlobalConnect has implemented controls to ensure that employees are qualified and conscious of their tasks and responsibilities in relation to information security.

People seeking employment at GCOS, must provide proof of personal criminal history. Operational staff with access to customer data are subject to security clearance by authorities equivalent to their access requirements.

Management's responsibility
Staff commit themselves, at their employment, to comply with the company's policies and rules, including the information security rules.

Awareness of information security, education and training
Staff are informed of all material changes to applicable policies and relevant procedures. This is done partly through the All-hands meetings in the and partly at periodic staff meetings.
GCOS also participates in the group-wide awareness programme.

Roles and responsibilities
The responsibilities of the staff follow their place in the organisation, which is described in the organisational chart, and where an increased responsibility applies this is described in the security policy.

Non-disclosure agreements
Confidentiality is part of the employment contracts.

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

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

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

Sanctions relating to breach of the information security
In addition to common employment law provisions, the general GlobalConnect staff manual specifies sanctions. The workplace is subject to GlobalConnects policies to which employees must be compliant. If a breach of policy happens, it could be considered a breach of the employment contract.

A.8 Asset management
GCOS has implemented controls to ensure achievement and maintenance of suitable protection of the organisation's equipment.

Registration of equipment
Relevant equipment, which is utilised, is registered in GCOS' CMDB in service desk system, in which all changes are also registered.

Accepted use of equipment
The employees' use of IT equipment and data is subject to fixed guidelines, defined in GlobalConnect's and GCOS' information security instructions, including but not limited to policies, directives, and rules.

Management of portable media
The rules for use of portable media are contained in the classification system described in the general information security policies, and in GCOS' information security rules.

Procedures for information management
All processing of data follows the guidelines set out in the classification system for GCOS.

A.9 Access management
GCOS 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 rescinded when the relevant access is no longer necessary.

Procedure for access control
As a supplement to our security rules, GCOS has a formal procedure for access management.

Guidelines for use of network services
All user rights, including access to network, drives and applications, are determined based on the users function.

Account provisioning
GCOS has procedures for the provisioning and deprovisioning of user accounts, which are placed in our service desk system in the form of workflows.

Extended rights
All rights are managed based on the employees' roles and are checked regularly in our quality management system. Extension of standard rights follows our formal access management procedure.

Management of password
Granting of passwords is subject to several rules which are set out in our identity management systems.

Reassessment of user access rights
All accesses and rights are reviewed periodically by the quality manager and the GCOS department managers.

User identification and authentication
GCOS has separate admin-profiles for all operational staff on the systems where this is technically possible. All password validation is made via Password Manager systems which manages validation of the individual logins.

A.10 Cryptography

GCOS has implemented controls to ensure correct and effective use of cryptography to protect confidentiality, authenticity and/or integrity of data.

Data traffic
Backup data, sent via dedicated lines to the organisation, are secured by one or more encryption keys.

A.11 Physical and environment security
GCOS has implemented controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

Physical access control
GlobalConnect premises have access control in the form of a required personal code and a physical access token, e.g., chipcard, to ensure that only authorised staff have access. Only GlobalConnect staff receives physical token and a code. If suppliers, consultants, or other external parties are to have access, this is only possible while accompanied by authorised personnel.

Safeguarding of offices, premises, and facilities
GlobalConnect premises have access control in the form of a required personal code and a physical access token, e.g., Chipcard, to ensure that only authorised staff have access.

Protection against physical external threats
We refer to separate a ISAE 3402 report on the description of controls, their design and operating effectiveness relating to GlobalConnect's Data Center solution.

Storing of equipment and protection of equipment
Critical equipment is placed in a server room to which only technical staff and GlobalConnect's partners have access.

A.12 Operations security
GCOS has implemented controls to ensure that operation of servers and key systems is carried out in a structured and secure manner.

Documented operating procedures
All operating procedures are included in GCOS' quality management system and are therefore easily available to all staff through our quality portal. They are all based on ITIL and generally integrated in our service desk system. The quality management system involves maintenance and minimum one annual review of all procedures.

Safeguarding of systems documentation
GCOS keeps the systems documentation centrally in our CMDB in service desk or other suitable repositories of documentation, depending on the nature of documentation, which can solely be accessed by authorised staff.

Control of procedures for changes
GCOS have a formal procedure for change management, which is based in our service desk system.

Management of capacity
Monitoring of capacity has been implemented and GCOS receives reporting from various tools, including monitoring software, which are used in the planning of purchase of additional capacity. Data from monitoring are registered and evaluated currently.

Backup of information

Backup is performed for all important data according to customer agreements made. Errors in backup are identified by the relevant backup management tools and registered in GCOS' service desk. Restore test for the customer is performed only when a specific agreement exists between the customer and GCOS.

Control of malicious code
All registered servers in GCOS' infrastructure are updated with approved antimalware, unless specific circumstances prevent this (e.g., due to application compatibility). When a new server is set up, workflows in GCOS' service desk ensure that antimalware is installed. All workstations in GCOS are updated with antimalware. New workstations are installed with a standard image, which contains antimalware.

Audit log
User transactions, exceptions and security incidents are logged, and the log is stored according to the retention periods according to company policy or as agreed with the customer.

Use of monitoring systems
GCOS has implemented internal procedures to ensure that alerts and alarms are addressed in order to respond to relevant incidents and act accordingly. All relevant alarms are shown on a big screen within normal working hours and to the on-duty officer during on-duty periods. This can also be monitored remote by Operations staff securely logging in. All alarms are reviewed continuously by GCOS' operations department and are reported to customers because cases are created on the basis hereof.

Logging of administrator and operator
System administrators' actions are logged automatically in our service desk system and in the relevant log-collection solutions as applicable by a specific system or platform.

Logging of errors
Monitoring has been set up for the purpose of future analysis of errors and incidents in our service desk.
A.13 Communications security
GCOS has implemented controls to ensure that operation of material infrastructure components is carried out in a structured and secure manner.

Network controls
GCOS has written procedures for configuration of firewalls, routers, and switches, which are solely carried out by the operations department.

Security services on the network
Access to GCOS' systems for our customers goes either through public networks where access is via VPN, MPLS or firewall. Access and communication between our servers and the internet go through our centrally managed firewall, where logging has been set up. All incoming network traffic goes through our redundant firewalls. Only approved network traffic is allowed through the firewall based on a customer request.

Policies and procedures for data exchange
All data exchanges are as a minimum encrypted, meaning that they go via VPN or SSL/TLS encryption.

Control of network connections
Customer networks are limited by the VLAN and Access rules in our Core router / firewall. It is solely approved GCOS personnel that can access the different customers' VLANs via the admin network physically on GCOS.

A.14 Acquisition, development, and maintenance of systems

GCOS has implemented controls to ensure that servers and relevant infrastructure components are updated and maintained as necessary and that this is done in a structured process.

Change management
GCOS has a formal Change Management procedure to ensure that systems are reassessed and tested in connection with major changes and follows the process in our service desk system in the form of formalised workflows. Security patches are applied at fixed intervals in the service windows agreed with the customers. All other service packs are installed solely at request, or by approval by the customer, following a recommendation by GCOS, and follows the process in our service desk system in the form of formalised workflows.

Control of technical vulnerabilities
Scanning for updates to systems is done using software tools. Hereafter, GCOS' formal procedure for patching is followed.

A.15 Supplier relationships
GCOS uses several technology vendors for different information processing services, these are managed and evaluated according to classifications of the services provided.

Management of security in agreements with third party
If the sub-suppliers are an integral part of our services, we inspect the controls implemented by the supplier by obtaining an ISAE 3402 auditor's report.

Relevant providers and consultants are to sign a non-disclosure agreement and confirm that they are familiar with our security policies and rules.

To the extent that GCOS' sub-suppliers store or otherwise manage personal data on behalf of GCOS' customers in the course of the sub-supplier's provision of services to GCOS, the sub-supplier acts as data processor solely according to instructions from GCOS and GCOS' customer. Thus, GCOS's sub-suppliers commit themselves to take the necessary technical and organisational security measures to ensure that personal data are not accidentally or illegally destroyed, lost or impaired, and that they are not disclosed to unauthorised parties, misused or otherwise processed in violation of data protection legislation.

A.16 Information security incident management
GCOS has implemented controls to ensure that security incidents are dealt with on a timely basis and that there is follow-up hereon.

All incidents, including security incidents, follow our formal Incident/Problem Management or Request Fulfilment procedure. These are included in our quality management system and bases in our service desk system.

The process includes, among others, receipt and registration, assessment and examination, escalation and troubleshooting, and restore of all incidents, if relevant. All priority-1 incidents are reported directly to our operations manager, project manager and other relevant managers. This is done automatically in our service desk system. Moreover, our quality management system has a formal procedure for escalation of all types of incidents, including security incidents.

A.17 Information security aspects of contingency, disaster recovery and restore management
GCOS has prepared a contingency plan which is updated as required.

Information security integrated in the contingency plan
GCOS has a formal contingency plan in which information security is incorporated.

Development and implementation of contingency plans which include information security
GCOS has developed contingency plans to maintain or restore operations and ensure access to data at the required level and within acceptable time after failure or outage of critical business processes.

Responsibilities and guidelines
Roles and responsibilities are defined in the contingency plan. The operations manager and the contingency managers are responsible for different areas.

Contingency plan
GCOS assesses risks regularly, and the contingency plan is updated to the existing risk exposure at least once a year in connection with Management's review and approval of the security policy.

Testing, maintenance, and reassessment of contingency plans
The contingency plan is tested annually to ensure that it is applicable, sufficient, and effective.

A.18 Compliance with customer requirements and regulatory and public authority requirements
GCOS has implemented controls to ensure that all relevant customer requirements and regulatory and public authority requirements are complied with.
Compliance
As part of the customers' onboarding into GCOS managed services, procedures have been implemented to ensure that all customer requirements have been identified and addressed. Thus, project management is used to manage the customers' implementation in GCOS' operations environment.

Independent assessment of the information security
A large part of the procedures and the underlying controls is part of our ISO 9001 certified quality management system which is, besides regular internal audits, also subject to annual external audit.

GCOS maintains a ISO 27001 certification regarding information security. As part hereof, procedures are prepared for an annual reassessment and approval of underlying policies, process and procedure descriptions and is audited annually.

Privacy and protection of personal data
GCOS stores and processes personal data as instructed by the customer for the customers who have made data processing agreements with us (we refer to our separate ISAE 3000 report for this area).

CHANGES TO SERVICES AND RELATING CONTROLS

In the period from January 1st to December 31st, 2023 no material changes were made to GlobalConnect's services within Outsourcing Services and relating controls.

SUPPLEMENTARY INFORMATION ON THE IMPLEMENTED CONTROL ENVIRONMENT

Conditions to be observed by the customers' auditors

To achieve the above specified control objectives, controls must be implemented and correctly managed by the user organisations, including but not limited to:

User administration
GCOS grants access to internal staff and manages the user administration. GCOS carries out user administration of customers' staff if an agreement has been made for this purpose. The user administration is carried out at the request of the customer. It is the customer's responsibility to ensure that GCOS receives the correct information in relation to the user administration.

Configuration of security
GCOS has implemented security on the network layer in the form of segmentation, requirements for password and logging. If the security on the customer servers is not configured by GCOS, it is the customers' responsibility to ensure security on servers hosted at GCOS. When GCOS installs servers, a baseline is used to ensure suitable security on the servers.

Disaster recovery
GCOS has implemented controls to ensure that backup is taken of data, and that the readability of the backup is checked regularly. If complete systems are to be restored, GCOS ensures that backup copies of data are available for the restore of the system where GCOS' customers are themselves responsible for restoring of the systems. If complete systems are to be restored and an agreement has been made for this purpose, GCOS will ensure that this is possible and will test this according to the agreement. GCOS' customers are responsible for ensuring that systems that are selected for backup, backup schedules and data retention plans for those systems are sufficient for the business needs of the customer.

Protection of equipment at GCOS' customers
GCOS has implemented controls for physical protection of equipment placed at GCOS, including equipment placed at GlobalConnects data center. Protection of the equipment includes, among others, restrictions on the physical access to the relevant equipment. GCOS' customers are responsible for physical safeguarding of equipment placed in their own physical environment.

** Limited responsibility **

Responsibility for compliance with the control objective is divided between Beierholm kunde ApS and the subcontractors.

See description of controls in relation to covering the control risk, including how Beierholm kunde ApS continually supervises operations security and data security.

CHAPTER 3:

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

For the customers of GlobalConnect A/S 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 Outsourcing Services, throughout the period 1 January 2023 - 31 December 2023, 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.

The report is based on a partial approach, which means that the present report does not include the IT security controls and control activities related to the use of external business partners. The report does not include control or supervision of subcontractors in relation to Outsourcing Service activities. GlobalConnect A/S' subcontractors are listed in the Data Processing Agreements with the customers.

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2.

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 ISQM 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 GlobalConnect Outsourcing Services, such as this control environment was designed and implemented throughout the period 1 January 2023 - 31 December 2023 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 2023 - 31 December 2023; 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 2023 - 31 December 2023.

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, 30 January 2024

Beierholm
State Authorized Public Accountants
CVR 32 89 54 68

Kim Larsen
State-authorized Public Accountant

Peter Nicolai Riis
IT-auditor

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 2023 - 31 December 2023.

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 inspected 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. The policy is reassessed at planned intervals.	We have inspected GlobalConnects latest IT-security policy. Through the audit we have checked that the policy is maintained on a forthrunning basis 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	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. We have inspected documentation that supports the control activities.	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 management and acquired relevant documentation. We have inspected that the information security policy is maintained.	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 inspected 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 inspected relevant documentation that supports the control activity.	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 inspected documentation that supports the control activity.	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.
Updated antivirus must be installed on all mobile units used for work-related purposes.	We have interviewed relevant staff and management. The technical setup that ensures the control has been inspected and explained.	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 a criminal record can be shown.	We have interviewed relevant staff at GlobalConnect. We have inspected the recruitment 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 planning and performing documentation.	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 inspected 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. We have been inspected that it is required that employees sign an NDA as part of their signing their employment contract with GlobalConnect.	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.	We have interviewed relevant staff at GlobalConnect. We have inspected the workflow and documentation.	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 and documentation.	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 and documentation.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE 8:

Asset Management

Necessary protection of the company's information assets must be ensured and maintained, all the company's physical and functional assets related to information must be identified, and a responsible owner appointed. The company must ensure that information assets related to cloud-based ERP system have an appropriate level of protection.

There must be reassuring controls to ensure that data media are properly disposed of when no longer needed, in accordance with formal procedures.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
All equipment relevant to provision of services is identified and recorded in CMDB, in which changes are also recorded.	We have interviewed relevant staff at GlobalConnect. We have inspected registrations in the CMDB. We have inquired as to how it is ensured that relevant equipment is registered in the CMBD.	During our test, we did not identify any material deviations.
All customer IT equipment has been designated an owner.	We have interviewed relevant staff at GlobalConnect. We have inspected that relevant equipment is registered in the CMDB with an owner.	During our test, we did not identify any material deviations.
Guidelines are prepared for classification of information and data. All processing of media and data are performed according to GlobalConnect's classification system.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation in the form of guidelines.	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 inquired and inspected the security model and its implementation.	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. We have inquired to and walked through the process and its tasks at meetings. We have inquired relevant functions how Change is part. We have inspected documentation.	During our test, we did not identify any material deviations.
GlobalConnect grants access to network and network services according to the "need-to-know" principles (access according to function).	We have interviewed relevant staff at GlobalConnect. HR are responsible for the initial manager approved workflow which feeds the basic access requirements. We have performed a walk-through of the security model and its implementation.	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. We have inspected that HR are responsible for the initial manager approved workflow which feeds the basic access requirements. We have inspected documentation.	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. We have inquired and inspected the security model and its implementation.	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. We have inspected the process and documentation.	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.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
GlobalConnect has implemented logging of accesses with privileged accounts (administrative rights).	We have interviewed relevant staff at GlobalConnect. We have inquired and inspected the security model and its implementation. We have inspected documentation.	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. We have inspected documentation.	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. We have inspected documentation.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.10:

CHRYPTOGRAPHY

The control objective is to ensure the correct and effective use of cryptography to ensure confidentiality, authenticity and/or integrity of information.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
Processes and procedures are implemented for creation and maintenance of encryption keys for the customers who have specified the need in their contract with GlobalConnect.	We have interviewed relevant staff at GlobalConnect and inspected relevant documentation.	During our test, we did not identify any material deviations.
Backup data transmitted to GCOS are secured by TLS/SSL certificates.	We have interviewed relevant staff at GlobalConnect and inspected relevant documentation.	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 physical perimeter is established in accordance with the security requirements deemed necessary.	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: • Inspected that there are fire extinguishing systems installed as well as cooling in the datacenters. • Reviewed and inspected maintenance documentation to confirm that UPS and diesel generators are maintained on a regular basis and tested. • During visits at the datacenters, we have inspected that maintenance and monitoring of UPS and diesel generators is performed. • Inspected for monitored climate control equipment in the datacenters. • Inspected that power and data cabling is protected. • Inspected that burglar alarms are mounted relevantly. • Inspected 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 inspected documentation.	During our test, we did not identify any material deviations.

Activities are recorded in the access control system in Operations.	We have interviewed relevant staff at GlobalConnect. We have performed on-site inspection in the operations. We have inspected 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 performed of external access cards that have not been used within the last six months.	We have interviewed relevant staff at GlobalConnect. We have inspected control documentation.	During our test we did not identify any material deviations.
Half-yearly review has been performed of internal access cards that have not been used within the last six months.	We have interviewed relevant staff at GlobalConnect. We have inspected control documentation.	During our test we did not identify any material deviations.
It is tested that the access control system ensures that only authorized persons have the necessary access.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation.	During our test we did not identify any material deviations.

CONTROL OBJECTIVE A.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 has implemented formal operating procedures, which are available to all users having a function-related need for insight.	We have interviewed relevant staff at GlobalConnect. Procedures and guides are in general available for staff with a functions-related need on internal platforms.	During our test, we did not identify any material deviations.
All changes to systems are managed and subject to the common change management process. Changes and management hereof are documented in Service Management System, in which the necessary approvals are registered.	We have interviewed relevant staff at GlobalConnect. We have performed a walk-through of the process and inspected documentation for the control.	During our test, we did not identify any material deviations.
Each change is subject to risk assessment and prioritised.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
Customers are warned before the change work is commenced to ensure least possible inconvenience for the customers.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
Monitoring and registration of customers' IT environment has been established for the customers who require management of the capacity to prevent system breakdown.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
GlobalConnect has separated IT environments into development, test and operating environments for the customers who require this.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.

All relevant entities in GlobalConnect's infrastructure are updated with approved malware software.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
Malware software is updated with the most recent version (signature file).	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
Backup of data is performed for all customers with backup agreements, some via sub-organisations and other internally in GlobalConnect.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
Restore tests are carried out for customers with restore agreements according to the agreements.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation.	During our test, we did not identify any material deviations.
Recording and managing of all relevant incidents has been established.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation. We have inspected registrations of incidents in the service management system and observed what is shown on different functions monitor screens as well as inquired about incident handling.	During our test, we did not identify any material deviations.
Monitoring of customers' servers has been established.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and documentation. We have inspected registrations of incidents in the service management system and observed what is shown on different functions monitor screens as well as inquired about incident handling.	During our test, we did not identify any material deviations.
Procedures are implemented to ensure that all activities performed by systems administrator or employees with administrative rights are recorded.	We have interviewed relevant staff at GlobalConnect. We have performed a walk-through of the security model from normal user to domain admin and we have seen that	During our test, we did not identify any material deviations.

	monitoring and registration of activity is performed.	
Infrastructure components have been implemented which are time synchronised up to centralised NTP servers.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation for the control showing the NTP servers.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.13:

COMMUNICATION SECURITY

To ensure protection of information in networks and support of information processing facilities.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
Formal business procedures have been implemented to safeguard internal and external transfers of confidential or sensitive information or data, where required.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation for the control.	During our test, we did not identify any material deviations.
Remote access has been established to GlobalConnect's systems for customers requiring this. The access is either through public networks, protected by VPN or MPLS and firewall.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation for the control.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.14:

SYSTEM ACQUISITION, DEVELOPMENT AND MAINTENANCE

Ensure that software development related to system solutions is managed using suitable IT control measures, including appropriate segregation between production and development environment.		
GlobalConnect's control procedures	Auditor's test of controls	Test findings
Formal processes and procedures have been implemented for all changes made in the company's own IT environment.	We have interviewed relevant staff at GlobalConnect. We have inspected the procedure for Change on the network and server environments and seen documentation.	During our test, we did not identify any material deviations.
Formal business routines and procedures for implementation of software in own and the customers' environments.	We have interviewed relevant staff at GlobalConnect. We have inspected the procedure for projects and Change and inspected documentation.	During our test, we did not identify any material deviations.
Formal processes and procedures (Patch Management) have been implemented for security updates of operating systems.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and inspected documentation for the control.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.15:

SUPPLIER RELATIONSHIPS

External business partners are obliged to comply with the company's established framework for IT security level.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
All relevant service organisations have signed an NDA with GlobalConnect and are familiar with the content of our security manual.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and inspected documentation for the control.	During our test, we did not identify any material deviations.
Business procedures have been established to ensure supervision of GlobalConnect's implemented controls in the form of obtaining an ISAE 3402 auditor's report.	We have interviewed relevant staff at GlobalConnect. We have inspected the process and inspected documentation for the control.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.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 process and inspected documentation for the control.	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 inspected the process and inspected documentation for the control.	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 inspected the process and inspected documentation for the control.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.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 relevant functions to ensure business continuance in connection with security incidents.	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 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. We have inspected documentation for the yearly test.	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. We have inspected documentation for the yearly test.	During our test, we did not identify any material deviations.
Redundancy has been established in relevant systems for the customers requiring this to meet availability requirements.	We have interviewed relevant staff at GlobalConnect. We have inspected documentation for the redundant setup.	During our test, we did not identify any material deviations.

CONTROL OBJECTIVE A.18:

COMPLIANCE WITH LEGAL AND CONTRACTUAL REQUIREMENTS

Procedures and controls are complied with to ensure that legal, public authority or contractual requirements are performed in accordance with the agreements.

GlobalConnect's control procedures	Auditor's test of controls	Test findings
GlobalConnect has identified all relevant legal and public authority requirement.	We have interviewed relevant staff at GlobalConnect. We have inspected that GlobalConnect has identified all relevant requirements.	During our test, we did not identify any material deviations.
GlobalConnect is ISO9001 and ISO27001 certified. As a part hereof, procedures are drawn of for an annual reassessment and approval of descriptions of underlying policies, processes, and procedures.	We have interviewed relevant staff at GlobalConnect. We have inspected that GlobalConnect Outsourcing Services hold the certifications in both standards.	During our test, we did not identify any material deviations.

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

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

Peter Nicolai Riis
BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 32895468
IT-auditor
Serienummer: 135ccee6-9c8d-426c-bec0-ba9ff5898423
IP: 212.98.xxx.xxx
2024-02-16 08:04:13 UTC

Kim Holm Larsen
BEIERHOLM, STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 32895468
Statsautoriseret revisor
På vegne af: Beierholm
Serienummer: bff7239f-6800-4339-865f-dbc13a357020
IP: 212.98.xxx.xxx
2024-02-16 15:29:53 UTC

Monika Juul Henriksen
GLOBALCONNECT A/S CVR: 26759722
Senior Vice President, Head of Nordic Enterprise
Serienummer: 8a8a0a1a-bff0-4e7d-96b9-46f32ed2e07c
IP: 217.61.xxx.xxx
2024-02-19 12:49:45 UTC