www.pwc.dk

Cloud Factory

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2023 to 31 December 2023 in relation to Cloud Factory's IT operations and hosting activities to customers

April 2024

Contents

1 Management's statement

The accompanying description has been prepared for customers who have used Cloud Factory's IT operations and hosting activities and the customers' auditors who have a 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 in the customers' financial statements.

Cloud Factory uses GlobalConnect A/S for housing of the primary and secondary data centres. This report uses the carve-out method and does not comprise control objectives and related controls that GlobalConnect A/S performs for Cloud Factory.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

Cloud Factory confirms that:

a) The accompanying description in section 3 fairly presents Cloud Factory's IT operations and hosting activities that have processed customers' transactions throughout the period from 1 January 2023 to 31 December 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to Cloud Factory's IT operations and hosting activities were designed and implemented, including:

   - The types of services provided
   - The procedures, within both information technology and manual systems, by which the IT general controls were managed
   - Relevant control objectives and controls designed to achieve those objectives
   - Controls that we assumed, in the design of Cloud Factory's IT operations and hosting activities, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
   - How the system dealt with significant events and conditions other than transactions
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to Cloud Factory's IT operations and hosting activities during the period from 1 January 2023 to 31 December 2023

   (iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to Cloud Factory's IT operations and hosting activities being described, while acknowledging that the 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 IT general controls in relation to Cloud Factory's IT operations and hosting activities that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2023 to 31 December 2023. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2023 to 31 December 2023.

Varde, 16. april 2024
Cloud Factory

Jacob V. S. Schmidt, CEO

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2023 to 31 December 2023 in relation to Cloud Factory's IT operations and hosting activities to customers

To: Cloud Factory, Cloud Factory's customers and their auditors

Scope

We have been engaged to provide assurance about Cloud Factory's description in section 3 of its IT general controls in relation to its IT operations and hosting activities which have processed customers' transactions throughout the period from 1 January 2023 to 31 December 2023 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Cloud Factory uses GlobalConnect A/S for housing of the primary and secondary data centres. This report uses the carve-out method and does not comprise control objectives and related controls that GlobalConnect A/S performs for Cloud Factory.

Some of the control objectives stated in Cloud Factory's description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with Cloud Factory's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

Cloud Factory's responsibilities

Cloud Factory is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on Cloud Factory's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we plan and perform our procedures to

PricewaterhouseCoopers Statsautoriseret Revisionspartnerselskab, CVR no. 33 77 12 31
Strandvejen 44, DK-2900 Hellerup
T: +45 3945 3945, F: +45 3945 3987, www.pwc.dk

obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its IT operations and hosting activities and about the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the6escryption, the suitability of the objectives stated therein, and the suitability of the criteria specified and described by Cloud Factory in the Management's statement section.

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

Limitations of controls at a service organisation

Cloud Factory'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 hosting services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation 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 a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to Cloud Factory's IT operations and hosting activities were designed and implemented throughout the period from 1 January 2023 to 31 December 2023;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2023 to 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, operated effectively throughout the period from 1 January 2023 to 31 December 2023.

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used Cloud Factory's IT operations and hosting activities and their auditors who have a sufficient understanding to consider it, along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatements in their financial statements.

Aarhus, 16. april 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State Authorised Public Accountant
mne26801

Martin Roursgaard Nielsen
Manager

3 Service vendors system description

3.1 Introduction

This description is intended to give information for Cloud Factory partners and their auditors based on the International Auditing Standard for Service Provider Assurance Tasks, ISAE 3402. The description covers information about the system and control environment in place for Cloud Factory's operating and hosting services that are used for Cloud Factory's shared solutions.

This description explains the processes that are used to ensure the secure operation of systems. The goal is to provide enough information to help the partners' auditors independently evaluate the risk identification of control gaps in the control environment as part of the auditor's audit planning in 2023.

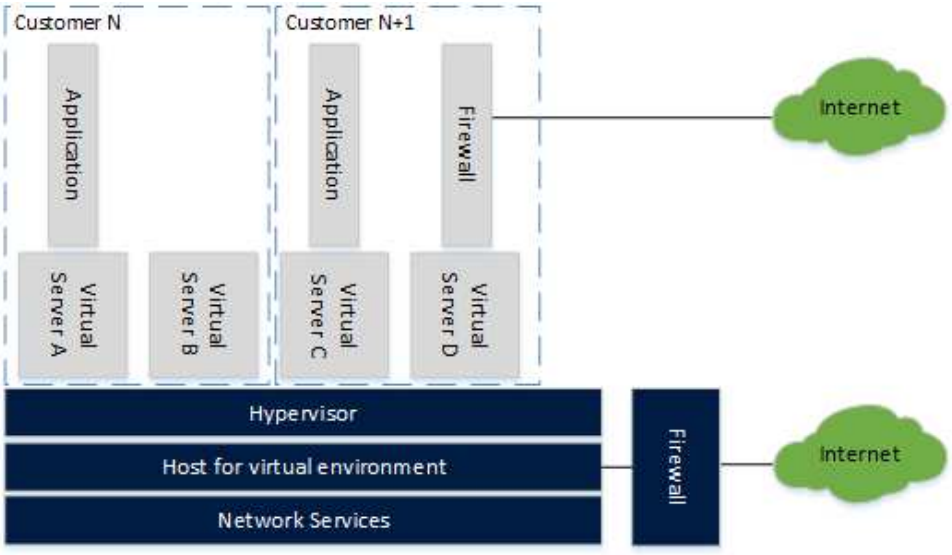
3.2 Description of Cloud Factory's services

Cloud Factory is a Danish company based in Denmark, but with sales offices in Norway, Sweden and the Netherlands. We work as a distributor of cloud services, mainly serving partners, such as Managed Service Providers (MSPs) and Independent Software Vendors (ISVs), and we do not deal directly with end customers.

As a cloud aggregator, we exclusively provide cloud services through our self-service portals: Partner Portal and Customer Portal. We have a broad range of cloud services and focus on delivering Infrastructure as a Service (IaaS) through our hyperconverged infrastructure platform.

Our IaaS product enables partners to buy and manage virtual machine system resources. We offer a simple and flexible solution where our partners can decide what they install on their virtual machines. Besides the infrastructure, we also give access to our underlying network as well as the choice to use our recommended firewall solution or install their own firewall.

Cloud Factory's IaaS product is different from a conventional hosting structure, as Cloud Factory provides the technical platform that partners can use to create their hosting business. This can be shown like this:



The blue areas are what Cloud Factory delivers and takes care of, while the gray areas are what the partners deliver and take care of.

Our self-service portal lets partners adjust their infrastructure as their business changes and gives a smooth and effective solution for buying and managing cloud services.

Cloud Factory offers dependable, high-quality cloud services that support digital transformation and enhance our partners' business results.

This statement does not include the outcomes and duties of IT hosting companies/partners.

3.3 Responsibility and organization at Cloud Factory

Cloud Factory has in 2023 been owned by Jacob V. Schmidt ApS, Mark R. Ibsen ApS and CF SPV ApS and employs approx. 40 employees. Product liability is located as follows:

- CEO (Chief Executive Officer), responsible for sales, marketing, purchasing, new development, etc.
- COO (Chief Operations Officer), partner contracts, SLA, risk management, etc.
- CFO (Chief Financial Officer), responsible for finance.
- CTO (Chief Technical Officer), responsible for engineering, monitoring, operations, support, etc.

Cloud Factory uses a few subcontractors to perform very specific tasks. The following areas are Cloud Factory's responsibility, but the daily tasks/security measures are handled by the following subcontractors:

- Housing of primary and secondary data centers is outsourced partly to GlobalConnect A/S and Bulk Data Centers Dk01 ApS.

3.4 Risk management at Cloud Factory

Cloud Factory follows certain procedures to evaluate the risks of its business. The IT risk assessment aims to reduce the risks related to the services that Cloud Factory offers to a tolerable level. The IT risk assessment is reviewed regularly and whenever new services are launched. The IT risk assessment is done by the managers of each department and other relevant staff and approved by Cloud Factory's Head of Governance and Compliance.

3.5 Control framework, control structure and criteria for control implementation

Cloud Factory has an IT security policy that covers all employees and that aims to ensure the proper and secure operation of Cloud Factory's main services that are offered to the partners. The IT security policy also involves ongoing enhancement of both physical and logical security, operational performance, contingency planning and support of the IT infrastructure, as well as implementation and documentation of the agreed controls.

Cloud Factory follows a control framework based on ISO 27001:2017 and best practices for reducing risks related to hosting services on shared infrastructure. According to this control model, the system and control environment for the services is defined in the following selected control areas of ISO 27001:2017:

- Information security policies
- Organization of information security
- Staff safety
- Media Management
- Access management
- Physical security and environmental security
- Reliability
- Communication security
- Supplier service management.

Cloud Factory has set up managerial controls that make sure that the employees and the relevant subcontractors follow the established procedures. This is done by relevant subcontractors verifying that they adhere to the cooperation agreement and therefore Cloud Factory's IT security policy.

3.6 Established control environment

Cloud Factory has an overall goal of providing stable and secure IT operations to its partners. This objective is reflected in defined policies in these four areas:

- Risk policy: Processes have been established for ongoing risk assessment of the company's business. The purpose is to ensure that the risks associated with the services and services provided by the company are reduced to an acceptable level.
- IT Security Policy: The policy covers all employees and all deliverables. Policies, procedures and operational operations are regularly updated.
- Control procedures: Monitoring and support policies and procedures are in place to ensure that your company's deliveries are consistent and transparent.
- Information management: Cloud Factory protects the information and knowledge that is continuously built up through daily case management, maintenance of databases and development of new products and initiatives.

Below are the individual control areas, established procedures and controls described in more detail.

3.7 Information security policies

Purpose

Management has defined policies and guidelines based on an assessment of IT risks in Cloud Factory's business, including that policies and guidance have been communicated to the entire Cloud Factory and the company's subcontractors.

Information security procedures and controls applied

Cloud Factory has defined a wide range of written procedures to support the company's goal of providing stable and secure IT operations to its partners. Employees and relevant subcontractors are familiar with these procedures, and management follows up on compliance with the procedures and that they reflect daily life at Cloud Factory. Mentioned below are the essential documents.

Risk assessment

Cloud Factory has evaluated the potential risks. As part of this process, the Company has identified the essential assets and information assets that need to be protected from any loss or compromise of availability, confidentiality or integrity, either singly or in combination, for the organization's business operations to continue.

However, Cloud Factory's analytics are reduced to the following elements only:

- Impact assessment
- Probability
- Risk.

Risk assessment is updated in the event of changes in the company's circumstances, e.g. in the event of changed service deliveries. Assessment must take place at least once a year.

IT Security

Based on the results of the risk assessment, Cloud Factory has developed relevant policies and guidelines that are available to all Cloud Factory employees. These are continuously updated as needed. The following main areas are addressed in the IT Security document:

- Physical security: extensive access to offices, subcontractors and data-carrying equipment
- Logical security: Comprehensive access and privilege management and security parameter requirements

- Staff and subcontractors: Guidelines for handling IT security towards staff and relevant subcontractors upon recruitment and termination

- Preparedness: Guidelines for handling IT security breaches, critical incidents and preparedness for attacks on online systems.

3.8 Organization of information security

Purpose

Management has placed responsibility for operations and IT security and ensured that relevant information is made available to employees and subcontractors.

Internal organization procedures and controls applied

All responsibilities for information security are defined and distributed. There is a set procedure for creating and maintaining user roles to avoid unauthorized and unintended use, modification, and misuse of assets.

Relevant Cloud Factory vendors and partners are contractually obligated to comply with the company's IT security policy and to familiarize themselves with the changes if Cloud Factory updates the policy.

3.9 Staff safety

Purpose

Management has established guidelines for recruitment, retention and resignation of staff, including guidelines to ensure that competencies are maintained, and the company's IT security is complied with.

Applied procedures and controls in the field of personnel safety

Cloud Factory has established guidelines for managing staff. The following guidelines should be particularly highlighted:

Before employment

The employees' and partners' contracts describe the respective and the organization's responsibility for information security and that this is aligned with Cloud Factory's guidelines.

Any verification of the background of job candidates shall be carried out in accordance with relevant laws, regulations and codes of ethics. This applies both to Cloud Factory and to the company's partners.

During employment

Management requires all employees and contractors to maintain information security in accordance with Cloud Factory policies and procedures. All the organization's employees and relevant partners are continuously informed and made aware of Cloud Factory's information security through training and exercises.

After employment

Information security responsibilities and obligations, which also apply after termination or change of employment, are defined and communicated to the employee/supplier and enforced by the company.

3.10 Media Management

Purpose

Management has established guidelines for handling data-carrying media.

Procedures and controls applied in the field of data-carrying media

The company does not handle sensitive data on hand-held media such as USB drives and DVDs.

When physically transporting media with sensitive data, carrier must be used. The media must be protected against unauthorized access, misuse and destruction during transport.

When replacing outdated or damaged hard drives, the replaced hard drive will either be sent back to the supplier of the equipment in question for data clearing, alternatively Cloud Factory performs the replacement itself, and places the hard drive in a closed container handled by the company Marius Pedersen, which through our contract handles hard disk shredding in a professional manner.

3.11 Access management

Purpose

Management has established guidelines for managing access to Cloud Factory's system environments, including the granting of rights, so that an appropriate separation of incompatible functions is established.

Access management procedures and controls applied

Cloud Factory has set up rules for giving access and rights to the system environments they use.

Access to system environments is by using standard Microsoft authentication methods with unique user IDs and passwords. Password requirements follow best practice in Denmark.

Access is through the Internet. Access from the Internet to internal networks goes through firewalls.

All customer access, i.e. external user access, to each hosted environment is through VPN, Virtual Private Networks, as a direct connection over the Internet or via MLPS (Multiprotocol Label Switching) connection or via Console access in the Partner Portal.

Personal workstations at Cloud Factory have screensavers that need passwords to use.

All persons with access to Cloud Factory environments, including those employees who have theoretical access to or practical ability to read data in the environments of resellers and end customers, must sign a confidentiality agreement that commits to the confidentiality of any information that person may become aware of. The declaration applies both during and after the employment relationship. The confidentiality requirement applies:

- All employees
- All employees at subcontractors (with access to the company's IT systems).

It is the responsibility of Cloud Factory's management to monitor granted access and rights on a regular basis and to ensure that employees comply with the confidentiality statement and take action if violations occur.

3.12 Physical security and environmental security

Purpose

Management has established guidelines for managing access to Cloud Factory's physical facilities, including equipment placed with subcontractors.

Procedures and controls applied in the field of physical security measures

Cloud Factory has defined guidelines for safe physical security measures.

Access to offices

Physical access to Cloud Factory takes place outside normal opening hours with a key and access tag provided. Guests are always accompanied by a staff member.

Housing at subcontractors
Cloud Factory's servers are physically located at GlobalConnect and BULK for primary and secondary data centers, respectively.

It is the subcontractors' job to ensure a safe physical environment for Cloud Factory's hosting system and the company's partners' and end customers' data. Servers, services, data and other information are protected against damage from fire, water, temperature, power failure, vandalism, theft, etc.

The subcontractors have emergency power systems and diesel generators. There is redundant cooling and fire extinguishing systems. All equipment with Cloud Factory's customer data is placed in rack cabinets within locked fences.

Access to the server rooms is limited with access cards with associated code and some physical keys. Only authorized persons have access to the server rooms.

Housing of production
Servers are physically located at the housing supplier GlobalConnect A/S.

Access cards for the lease at GlobalConnect can only be issued upon approval and booking via named managers. Cloud Factory regularly follows up on which people have access to equipment at GlobalConnect A/S.

Access for technicians employed by subcontractors follows GlobalConnect's fixed procedures, and access is only granted by agreement with Cloud Factory in each case.

Guests are only allowed if accompanied by a staff member.

Cloud Factory receives an annual ISO27001 certificate and a 3402 declaration from GlobalConnect A/S on their security measures.

It should be emphasized that the physical security measures at GlobalConnect A/S are not part of this statement.

Housing af Disaster Recovery
Cloud Factory's Disaster Recovery is physically located at 2 different locations, by 2 different housing suppliers. For this purpose, GlobalConnect A/S and BULK data center DK01 are used.

Admission cards for the lease at GlobalConnect and BULK can only be issued upon approval and booking via naming managers. Cloud Factory regularly follows up on which people have access to equipment at GlobalConnect A/S and BULK data center DK01.

Access for technicians employed by subcontractors follows GlobalConnect and BULK's fixed procedures, and access is only granted by agreement with Cloud Factory in each case.

Guests are only allowed if accompanied by a staff member.

Cloud Factory receives an annual ISO27001 certificate and a 3402 declaration from GlobalConnect A/S on their security measures and an ISO 27001 from BULK data center DK01 on their security measures.

3.13 Reliability

Purpose
Management has established guidelines for ensuring adequate operational reliability in accordance with the company's IT security policy and agreements entered into with partners.

Operational safety procedures and controls applied

Cloud Factory has defined operating procedures that are made available to all users in need. The system documentation and the description of the internal routines are updated in the event of significant changes in operational processes and systems.

Management and monitoring of operations takes place in several different tools for monitoring operations, including monitoring that customers receive the contracted delivery. The following tools are used:

- PRTG – System Environment Monitoring Tool
- Atlassian Jira – Project and Task Management as well as
- Atlassian Status page – Sending notification to partners in case of maintenance or critical incidents
- Atlassian Confluence – Documentation and procedure descriptions.

Alarms from these tools are accessed by the technical department's operations group depending on the incident, so that there will always be an operations employee who can take care of any errors and alarms.

Logging and monitoring

Automated monitoring takes place around the clock. The process is followed by Cloud Factory operating staff, who receive the alerts and process them continuously.

The relevant system administrator actions, such as login attempts, changes to the core products' management systems are logged partly on the host servers, and partly in the administration tools provided by Cloud Factory. Logs are protected against unauthorized access and exported on a daily basis to external systems where they cannot be manipulated.

All configuration changes and updates in the equipment follow our Change Management procedure.

Critical incident management

Cloud Factory has tools and procedures for handling critical incidents, partly identified by the partners and partly by internal operational staff. These are handled based on set SLAs and regular management checks and staff training are carried out to ensure the set guidelines are followed by support and operational staff.

Operating software management

Procedures have been implemented to manage updating and maintaining the virtual environments.

Change control – patch management

Cloud Factory has devised a procedure to handle patches. This procedure is handled by the company's Infrastructure as a Service team and is documented in the internal operational documentation.

Change management

Cloud Factory has designed a procedure to handle changes. In connection with changes, a procedure has been developed for the approval of proposed changes. These are assessed by one or more of the technical staff in the Infrastructure as a Service team, and a senior executive, the manager, is the ultimate approver or rejector of the proposed changes.

When a change is accepted, a decision is made on what is required for it to be implemented. All this is documented in the internal operating documentation.

Vulnerability management

Cloud Factory continuously receives information about technical vulnerabilities, evaluates them and implements appropriate measures to manage the associated risk.

Disaster recovery

The Disaster Recovery solution is spread over 2 different geographical locations.

The first Disaster Recovery copy is placed on the production environment to achieve the fastest possible restore time if a partner's virtual system needs to be recreated. Here, a snapshot technology is used where

snapshots of all Virtual Machines are made every two hours, this copy is stored in 24 copies, i.e. 48 hours behind.
In addition, 1 additional snapshot is taken once a day, this is stored for 30 days.

The daily snapshot, which is stored for 30 days, is also sent to another geographical location, so there will be 2 copies of the daily snapshot at any time, divided into 2 geographical locations.

Regular testing is carried out to ensure that the restore can be completed. Cloud Factory is not responsible for in-guest backup of established servers, databases and applications that the individual partners may have installed on the shared infrastructure.

3.14 Communication security

Purpose
Management has established guidelines for managing networks and communications.

Procedures and controls applied in the field of communication security
Cloud Factory has designed procedures to handle patches, changes and critical incidents. These procedures are handled by the company's Infrastructure as a Service team and are documented in the internal operating documentation as mentioned above.

Cloud Factory has installed a firewall to protect the content on its own virtual servers and the infrastructure in general.

Cloud Factory's systems are set up so that no end customers share networks. Only select users in the Infrastructure as a Service team at Cloud Factory can log on to the critical network equipment.

Change control – patch management
Cloud Factory has devised a procedure to handle patches. This procedure is handled by the company's Infrastructure as a Service team and is documented in the internal operational documentation.

Change management
Cloud Factory has a method for managing changes. They have created a method for approving suggested changes related to changes. These are evaluated by one or more of the technical staff in the Infrastructure as a Service team, and a senior executive, the manager, has the final say on whether the suggested changes are approved or rejected.

When a change is approved, a decision is made on what is needed for it to be executed. All this is recorded in the internal operating documentation.

3.15 Supplier service management

Purpose
Management has established guidelines for managing subcontractors, including that they comply with the guidelines set at Cloud Factory.

Procedures and controls applied within suppliers
For each vendor that can access, process, store, communicate, or provide services to Cloud Factory, the company agrees on relevant requirements for the vendor's information security compliance.

Cloud Factory regularly monitors and reviews the supplier services received. Changes to supplier services, including the maintenance and improvement of existing information security policies, procedures and controls, must be managed taking into account the criticality of the business information involved and a reassessment of risks.

3.16 Complementary controls - Issues to be observed by the partners' auditors

Provision of services

The above system description of controls is based on Cloud Factory's Standard Terms of Agreement for IaaS services. The partners' own auditors should assess the applicability of this opinion and identify for themselves any other risks deemed material for the presentation of the partners' annual accounts. The same applies to a partner's customer – the "end customer".

Thus, the partners themselves must establish security measures and controls on the virtual environments, servers, databases and applications built on Cloud Factory's platform. Areas to be checked are the following:

- User management for servers, databases and applications
- Confidentiality on and around end customers' data
- Backup of servers, databases and applications
- Operational monitoring of servers, databases and applications
- Patch management and change management of servers, databases and applications
- Emergency management of servers, databases and applications.

The physical security measures at GlobalConnect A/S and BULK data center DK01

The partners' auditors should evaluate the risks associated with the physical security controls of the subcontractors and, if needed, request their ISAE 3402, ISO 27001 or similar report on their hosting environments.

Compliance with relevant legislation

Cloud Factory has set up processes and measures to ensure that the areas under its responsibility are handled securely. Cloud Factory does not have control over the servers, databases and applications that run on the shared infrastructure, and therefore, this statement does not cover the assurance that these systems have proper controls in place, or that the partners and their customers follow the Bookkeeping Act, the Personal Data Act or other applicable laws.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", and additional requirements applicable in Denmark.

Our testing of the design, implementation and functionality of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2 Test actions

The test actions performed when determining the operating effectiveness of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned during the period from 1 January 2023 to 31 December 2023. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

4.3 Overview of control objectives, control activity, tests and test results

A.5 Control objective: Information security policy

Purpose: To provide guidelines and support information security in accordance with business requirements and relevant laws and regulations.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
5.1.1	**Information security policies** Cloud Factory has established a written IT security policy which is maintained and approved by Management.	We made inquiries of Management about the procedures/control activities performed and reviewed the adequacy of the information security policy. We inspected that Management has approved the IT security policy.	No exceptions noted.
5.1.2	**Review of information security policies** Cloud Factory has established a written IT security policy which is maintained on an annual basis.	We made inquiries of Management about the procedures/control activities performed. We inspected that the IT security policy is reassessed at least once a year. We also inspected that the policy is easily accessible to the employees.	No exceptions noted.

A.6 Control objective: Organisation of information security

Purpose: To establish a management framework for initiating and managing the implementation and operation of information security in the organisation.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
6.1.1	**Information security roles and responsibilities** Cloud Factory has defined roles and responsibilities for material matters in its IT security document. Based on the size of the organisation, roles for the individual employees have been defined. However, Cloud Factory is characterised by its wide use of sub-suppliers for the actual execution of tasks.	We made inquiries of Management about the responsibilities with Management. We inspected that the organisational responsibility for material matters is documented in the IT security policy.	No exceptions noted.
6.1.2	**segregation of duties** Segregation of duties is in place; for example, not everyone is administrators, and access to central documents in the company's document management tool is restricted.	We made inquiries of Management about the procedures/control activities performed. We inspected access to the company's document management tool and users with administrative rights to verify that access is based on a work-related need.	No exceptions noted.

A.7 Control objective: Human resource security

Purpose: To ensure that employees understand their responsibilities and are qualified for their intended roles.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
7.1.1	**Screening** In its recruitment policy, Cloud Factory has defined requirements for verification of the qualifications of job candidates.	We made inquiries of Management about the procedures/control activities performed when verifying the qualifications of job candidates. We inspected the recruitment policy in relation to the set requirements for verification of qualifications. By inspection, we tested that screening of qualifications of job candidates is carried out.	During our test, we noted that the need for screening was not documented for 3 out of 3 samples. No further exceptions noted.

A.7 Control objective: Human resource security

Purpose: To ensure that employees understand their responsibilities and are qualified for their intended roles.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
7.1.2	**Terms and conditions of employment** In its recruitment policy, Cloud Factory has defined requirements for employees and sub-suppliers, respectively.	We made inquiries of Management about the procedures/control activities performed. We inspected the recruitment policy and inspected that control activities are adequate.	No exceptions noted.
7.2.1	**Management responsibilities** In its IT security policy, Cloud Factory has specified guidelines for the introduction of employees and business partners to Cloud Factory's information security guidelines.	We made inquiries of Management about the procedures/control activities performed. We inspected the IT security policy and inspected that control activities are adequate.	No exceptions noted.
7.2.2	**Information security awareness, education and training** In its IT security policy, Cloud Factory has specified guidelines for the awareness of employees and business partners with regards to Cloud Factory's information security.	We made inquiries of Management about the procedures/control activities performed. We inquired about information security management with Management. We inspected the latest initiatives within education and training relating to information security.	No exceptions noted.
7.2.3	**Disciplinary process** A formal and communicated disciplinary process must be in place to take action against employees who have committed an information security breach.	We inquired about the procedures/control activities performed. We inspected that a disciplinary process is in place and has been communicated to the employees to ensure that all employees are aware of the consequences of committing a security policy breach.	No exceptions noted.
7.3.1	**Termination and change of employment** On termination of employment, the employees' obligations with respect to secrecy and confidentiality are still covered by the contract.	We made inquiries of Management about the procedures/control activities performed in relation to the termination and change of employment. We inspected that employees are bound by secrecy and confidentiality through their contracts.	No exceptions noted.

A.8 Control objective: Asset management

Purpose: To prevent unauthorised publication, modification, removal or destruction of information stored on media.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
8.1.1	**Inventory of assets** Assets associated with information and information processing facilities must be identified, and an inventory of these assets must be drawn up and maintained.	We inquired about the procedures/control activities performed. We inspected that adequate controls are in place to ensure documentation and maintenance of the supply of assets.	No exceptions noted.
8.3.1	**Management of portable media** Cloud Factory has established guidelines for handling data storage media.	We made inquiries of Management about the procedures/control activities performed in relation to the management of portable media. We inspected the guidelines for handling data storage media.	No exceptions noted.

A.9 Control objective: Access control

Purpose: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
9.1.1	**Access control policy** An access control policy must be established, documented, and revised based on business and information security requirements.	We inquired about the procedures/control activities performed. We inspected that guidelines on access controls have been established, reviewed and approved.	No exceptions noted.
9.1.2	**Access to networks and network services** Users must only be provided with access to the network and network services that they have been specifically authorised to use.	We inquired about the procedures/control activities performed. We inspected on a sample basis that access to network and network services is granted based on the employees' job function and manager approvals.	No exceptions noted.
9.2.1	**User registration and de-registration** Cloud Factory has defined procedures for creation and deletion of users.	We inquired about the procedures/control activities performed in relation to creation and deletion of users. We inspected the procedures for user administration and inspected that control activities are adequate. By inspection, we tested the creations and deletions of users carried out during the period.	No exceptions noted.
9.2.3	**Management of privileged access rights** In its internal procedures, Cloud Factory has defined guidelines for granting privileged access and rights to employees.	We made inquiries of Management about the procedures/control activities performed. We inspected the procedures for user administration and inspected that control activities are adequate.	No exceptions noted.
9.2.5	**Review of user rights** Cloud Factory has defined a procedure for periodic review of users on a quarterly basis.	We inquired about the procedures/control activities performed in relation to periodic review of users. We inspected the procedures for user administration, including the IT security policy, and inspected that control activities are adequate. We have tested on a sample basis that quarterly reviews are carried out.	No exceptions noted.

A.9 Control objective: Access control

Purpose: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
9.4.2	**Secure log-on procedures** Access to systems and functionality is checked by authorisation functions in Microsoft systems. Access is handled through log-on to Windows domains, and rights are granted through association of security groups in Active Directory.	We inquired about the procedures/control activities performed in relation to secure log-on. We inspected the set-up of Windows Active Directory.	No exceptions noted.
9.4.3	**Password management system** Cloud Factory has defined a policy for the use of passwords.	We inquired about the procedures/control activities performed in relation to password management. We inspected the policy for the use of passwords.	During our testing, we noted that the system settings for lockout requirements are not in accordance with the recommendations on minimum requirements from the Danish Agency for Digital Government. No further exceptions noted.

A.11 Control objective: Physical and environmental security

Purpose: To prevent unauthorised physical access to, damage to and disruption of the organisation's information and information processing facilities.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
11.1.1	**Physical security perimeter** Security perimeters must be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. All of Cloud Factory's primary systems are located at GlobalConnect that houses servers and systems. Access to equipment is only granted following approval.	We inquired about the procedures/control activities performed in relation to physical access control.	No exceptions noted.
11.1.2	**Physical access control** Secure areas must be protected by appropriate access controls to ensure that only authorised personnel have access. All of Cloud Factory's primary systems are located at GlobalConnect that houses servers and systems. Access to equipment is only granted following approval.	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that access to Cloud Factory's equipment at the sub-supplier's premises is restricted to authorised personnel.	No exceptions noted.
11.1.3	**Securing offices, rooms and facilities** Physical securing of offices, rooms and facilities must be designed and applied.	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that Cloud Factory has implemented appropriate access controls to protect the physical facilities.	No exceptions noted.
11.2.1	**Equipment siting and protection** Equipment must be sited or protected to reduce the risk of environmental threats and hazards and the risk of unauthorised access.	We inquired about the procedures/control activities performed. We inspected that Cloud Factory has established guidelines for protection against fire, water and heat. We furthermore inspected that Cloud Factory has obtained an audit report from the sub-supplier in order to ensure that similar requirements are met in areas subject to outsourcing.	No exceptions noted.

A.12 Control objective: Operational security

Purpose: To ensure correct and secure operations of information processing facilities and to protect against loss of data.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
12.1.1	**Documented operating procedures** Cloud Factory has established written operating procedures for its core business.	We made inquiries of Management about the procedures/control activities performed.	No exceptions noted.
12.1.2	**Change management** Cloud Factory has defined a procedure for change management which is used for all changes that require test and/or service windows.	We inquired about the procedures/control activities performed, reviewed the adequacy of the change management procedures and inspected that an appropriate change management system has been implemented and is supported by technical infrastructure. Through an inspection of random samples of changes, we inspected the following: • Change requests are registered in the established system. • Documented test of changes, including approval • segregation of duties • Approval obtained prior to implementation.Where relevant, the plan for rollback is documented.	No exceptions noted.
12.3.1	**Information backup** Backup copies of information, software and system images must be taken and tested regularly in accordance with an agreed backup policy.	We inquired about the procedures/control activities performed in relation to backup. We inspected that requirements regarding backup have been established in the contract with sub-suppliers providing services for which backup is relevant. We inspected that a full restore test of IT environments has been performed.	No exceptions noted.

A.12 Control objective: Operational security

Purpose: To ensure correct and secure operations of information processing facilities and to protect against loss of data.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
12.4.1	**Event logging** Cloud Factory has defined a procedure for monitoring of operations. The monitoring covers internal events in the operations department. Furthermore, it includes alerts from the applied system environments. System environments are continuously monitored, and Management follows up to ensure compliance with Cloud Factory's guidelines. Currently, logging of traffic through firewalls is not implemented.	We inquired about the procedures/control activities performed in relation to event logging. We inspected the procedure for monitoring of operations as well as the documentation for monitoring of events.	No exceptions noted.
12.4.2	**Protection of log information** Log files currently placed at Cloud Factory are protected by password.	We inquired about the procedures/control activities performed in relation to protection of log information. We inspected that log files are protected by password.	We noted that logging is not adequately protected in terms of integrity and availability. No further exceptions noted.
12.4.3	**Administrator and operator logs** Logging of administrator actions has been set up, and the operator log is reviewed regularly.	We inquired about the procedures/control activities performed in relation to administrator and operator logs. We inspected that logging of administrator actions has been set up and that the operator log is reviewed regularly.	During our testing, we noted that the implemented logging does not align with PwC's best practices for administrator and operator logging. No further exceptions noted.
12.4.4	**Clock synchronisation** The clocks of all relevant information processing systems within an organisation or security domain must be synchronised to a single reference time source.	We inquired about the procedures/control activities performed. We inspected that Cloud Factory has established a reference time source for clock synchronisation of all relevant information-processing systems.	During our testing, we noted that one of the primary switches is not configured with clock synchronisation. No further exceptions noted.

A.12 Control objective: Operational security

Purpose: To ensure correct and secure operations of information processing facilities and to protect against loss of data.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
12.5.1	**Installation of software on operational systems** Procedures must be implemented to control the installation of software on operational systems.	We inquired about the procedures/control activities performed. Using random samples from the systems used to document changes, we examined whether – in accordance with guidelines – changes in the operating environment are carried out using a controlled process, including whether: • an approved test is performed before the changes are implemented. • testing and approval of emergency changes to the operating environment are documented immediately after implementation.	During our testing, we noted that there is no formalised procedure or technical measures for checking software. No further exceptions noted.
12.6.1	**Management of technical vulnerabilities** Cloud Factory has defined procedures for patch management. Testing of the firewall and its ability to withstand attacks is performed regularly.	We inquired about the procedures/control activities performed in relation to management of technical vulnerabilities. We inspected the procedure for patch management as well as the documentation of regular testing of the firewall and its ability to withstand attacks.	No exceptions noted.

A.13 Control objective: Communications security

Purpose: To ensure protection of information in networks and of supporting information processing facilities.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
13.1.1	**Network controls** Networks must be managed and controlled to protect information in systems and applications.	We inquired about the procedures/control activities performed. As part of our inspection, we have examined whether – in accordance with guidelines – an appropriate security architecture has been established in the network, including whether: • the network is segregated into secure zones and whether customer environments are separated from Cloud Factory's own environment • remote access is granted through two-factor authentication • changes to the network environment included in our tests are made in a controlled manner in accordance with the change management rules.	No exceptions noted.
13.1.3	**Segregation in networks** Groups of information services, users and information systems must be segregated on networks.	We inquired about the procedures/control activities performed in relation to segregation of duties. We inspected the technical security architecture, and we examined on a sample basis whether – in accordance with guidelines – an appropriate security level has been established, including whether: • secure zones and customer environments are separated from Cloud Factory's own environment • access to the network is segregated into relevant user groups based on users' work-related needs.	No exceptions noted.

A.15 Control objective: Supplier relationships

Purpose: To prevent unauthorised publication, modification, removal or destruction of information stored on media.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
15.1.1	**Contact to business partners** In its recruitment policy and its IT security document, Cloud Factory has defined requirements for information security when using sub-suppliers. As a rule, external business partners must comply with the same rules as Cloud Factory's employees, including the IT security policy. When concluding a cooperation agreement, this is pointed out to the sub-supplier.	We inquired about the procedures/control activities performed. We inspected the recruitment policy and the IT security policy in relation to the set requirements for compliance with the same rules as those that apply to Cloud Factory's employees. By inspection, we tested contracts with suppliers and business partners.	No exceptions noted.
15.1.2	**Addressing security within supplier agreements** Cloud Factory has concluded written agreements with external sub-suppliers. Every year, Cloud Factory receives a 3402 report for services delivered by external sub-suppliers.	We inquired about the procedures/control activities performed in relation to addressing security within supplier agreements. We inspected written agreements with external sub-suppliers.	No exceptions noted.

A.16 Control objective: Information security incident management

Purpose: To prevent unauthorised publication, modification, removal or destruction of information stored on media.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
16.1.1	**Responsibilities and procedures** Management's responsibilities and procedures must be established to ensure a rapid, effective and orderly response to information security incidents.	We inspected that a formal and documented incident management process has been implemented. We inspected that a formal and documented incident management process has been reviewed and approved. We inspected that the incident management process has been communicated to employees. We inspected that all incidents have been registered, that necessary actions have been performed and that the solutions have been documented in an incident management system.	No exceptions noted.

A.17 Control objective: Information security aspects of business continuity management

Purpose: To prevent unauthorised publication, modification, removal or destruction of information stored on media.

No.	Service organisation's control activity	Tests performed by PwC	Result of PwC's tests
17.1.1	**Planning information security continuity** The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	We inspected that a formal and documented business continuity plan is maintained, revised and approved annually. We inspected that a business impact assessment has been carried out to determine the requirements for a business continuity plan. We inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No exceptions noted.
17.1.2	**Implementing information security continuity** The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	We inspected that the underlying procedures have been implemented in the organisation. We confirmed through inquiry with relevant personnel that the employees have an understanding of the controls in relation to information security continuity.	No exceptions noted.
17.1.3	**Verify, review and evaluate the information security continuity** The organisation shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	We inspected that underlying procedures for the business continuity are reviewed and updated. We inspected that the underlying procedures have been tested to ensure that they are valid and effective during adverse situations.	No exceptions noted.

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."

Jacob Vestergaard Schaumann Schmidt
Kunde
Serienummer: 860e9b43-f2fe-412a-9e6a-fb8be3c54903
IP: 46.32.xxx.xxx
2024-04-16 15:02:43 UTC

Martin Roursgaard Nielsen
PwC-medunderskriver
Serienummer: 6698b5b9-6214-4759-bbe2-7140fb0c3b07
IP: 87.49.xxx.xxx
2024-04-16 15:18:34 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2024-04-16 15:26:12 UTC