Independent service auditor's assurance report on the description of controls, their design and operating effectiveness regarding any.cloud's operation of hosted services for the period 01-12-2018 to 30-11-2019

ISAE 3402-II

any.cloud A/S

CVR-nr.: 31 16 15 09

March 2020

Table of contents

Section 1: any.cloud A/S' statement

This description has been prepared for customers who have made use of any.cloud A/S' hosting services, and for their auditors who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements. any.cloud A/S confirms that:

(a) The accompanying description in Section 2 fairly presents any.cloud A/S hosting services related to customer transactions processed throughout the period 01-12-2018 to 30-11-2019. The criteria for this statement were that the included description:

(i) Presents how the system was designed and implemented, including:

- The type of services provided, when relevant, including processed groups information, when relevant
- The procedures, within both information technology and manual systems, by which transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to the customers
- Relevant control objectives and controls, designed to achieve these goals
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that were considered relevant to processing and reporting customer transactions.

(ii) Provides relevant details of changes in the service organization's system throughout the period 01-12-2018 to 30-11-2019.

(iii) Does not omit or distort information relevant to the scope of the described system, 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 system that each individual customer may consider important to their particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 01-12-2018 to 30-11-2019. 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

(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 01-12-2018 to 30-11-2019.

Copenhagen, 20 March 2020

any.cloud A/S

Gregor Møller
CEO

Section 2: any.cloud A/S' description of controls in relation to their hosting services.

Introduction

The purpose of this description is to inform any.cloud A/S' customers and their auditors about the requirements listed in the international standard on assurance engagements regarding assurance reports on controls at a service organization, ISAE 3402.

Moreover, the purpose of this description is to provide information about the controls used for cloud services with us throughout the period.

The description includes the control objectives and controls at any.cloud, which include our customers and is based on our standard delivery.

any.cloud provides professional ISO-compliant cloud, consultancy- and security services to companies both domestic and abroad. Any.cloud A/S' Danish infrastructure is hosted in InterXion Danmark, in Ballerup and Valby. Any.cloud has additional hosting services in the IBM Cloud-datacenters delivering services from more 60 datacenters, spread over more than 28 countries, which makes any.cloud A/S and international company, delivering services worldwide.

Through recent years, any.cloud has not only expanded and upscaled the business and the organization preparing for the increasing international demand, but also in terms of quality, the company has been undergoing significant changes.

Due to persistent re-certification through Danish Cloud Community, any.cloud has for several years been amongst the best hosting providers, leading through its accredited ISO27001-certification. any.cloud is committed to delivering according to strict controls, high security requirements and transparency in terms of quality and security in IT hosting services. This ensures that we constantly are maintaining the quality required for us to belong to the absolute elite within IT-solutions.

any.cloud has through many years obtained an ISAE 3402 Type II assurance report.

Any.cloud delivers the highest quality of IT outsourcing through the best suppliers and presents this to our customers my means of simple and innovative solutions. Through scalable business continuity, financial transparency and the willingness to take responsibility for the environmental aspects of doing business, we contribute to our customers' business and growth. We differentiate ourselves from other players on the market by means of our simple pricing policy, high quality, international presence, focus on the personal relationship, and our direct access to specialists, meaning that we have a very short response time.

The very special thing about any.cloud is that the customers experience high quality and transparency. Our business material constitutes a simple and transparent basis for decisions, and we serve our customers locally around the world. As a whole, any.cloud's customers experience a safe and close collaboration through an empathetic and personal relationship with our employees.

We are a strong international team, with offices in several countries.

Our goal is that the customer can focus on their business. We support and operate IT for companies and their employees, ensuring that they can always work - safely, efficiently and at a very favorable price.

Organization and responsibility

any.cloud has a clear and transparent corporate structure. Management is divided into four roles, Their roles and responsibilities are as described below:

CEO

Overall responsible for any.cloud, its condition and management. Furthermore, CEO is responsible for any.cloud A/S' marketing department.

COO

Responsible for operations, infrastructure, consultants, customer service, First line and development.

CFO

Responsible for any.cloud A/S' finances and financial staff.

CSO

Responsible for sale of all products, and sales staff.

Risk assessment

IT-risk analysis

We have procedures in place for on-going assessment of our business, especially our cloud services. This enables us to ensure that the risks associated with the services we provide are minimized to an acceptable level.

Risk assessment is performed periodically and when we introduce changes or implement new systems that we deem relevant in relation to re-performing our general risk assessment.

The company's COO is responsible for the risk assessments and they must subsequently be embedded and approved by management.

Management of security risks

Procedure for risk management

We have introduced points systems on the risks associated with providing cloud services. We use the calculation risk * impact with a score from 1-10. The acceptable level is maximum 30 points. We continuously assess whether we can reduce risks and take measures that can improve our score.

Information security policy

IT security policy document

We have defined our quality and control management system according to our overall objective of delivering stable and secure hosting and cloud services to our customers. To do that, we have necessarily introduced policies and procedures that ensure that our deliveries are uniform and transparent.

Our IT Security Policy is prepared with reference to the above and applies to all employees and to all deliveries.

Our method for implementation of controls is defined according to ISO 27002 (Code of practice for information security controls), and is overall divided into the following control areas:

- Organization and responsibility
- Human resource security
- Logical access management
- Risk assessment and management
- Physical security
- Use of IT equipment
- Operational procedures
- Network
- Support
- Protection against malicious software
- Acquisition and maintenance of systems
- Partners, including:
  - IBM Cloud
  - Microsoft Azure
  - InterXion
- Business continuity management

We are ISO 27001 certified and we are continuously improving policies, procedures, production together with physical and logical security.

Assessment of the IT security policy

We regularly update the IT security policy, as a minimum once a year.

Internal organization

Delegation of responsibility for information security

We have a clearly defined organization regarding delegation of responsibilities; and we have comprehensive descriptions of responsibilities and roles at all levels, from management to each individual operations employee.

We have established confidentiality in general for all parties involved in our business. This is done via employment contracts.

Segregation of duties

Through continuous documentation and processes we ensure that we can eliminate or minimize key staff dependency. Tasks are assigned and established via procedures for operations management.

Contact with special interest groups

We have established contact to a hotline at DK-CERT with whom we have entered a mutual agreement on notification in case of material security related matters regarding Internet traffic. Through our memberships with our primary partners, we also receive information about new vulnerabilities which may be relevant for our operations management.

Information security as part of project management

If we assess that a project does not comply with our information security, the project will be adapted to comply with our standard of information security accordingly. If we consider that the project cannot be completed or changed without violating our security policy, the project will be discarded.

Mobile devices and teleworking

Mobile devices and communication

We have implemented the possibility for our employees to work from home due to, amongst others, being on call in relation to operations and our policy is that devices (laptops, etc.) may only be used for work-related purposes and must not be left unattended, etc. Portable devices are protected with logon and encryption.

We have enabled that we and our customers can use mobile devices (smartphones, tablets, etc.) for synchronizing mails and calendars. Besides password protection, we have enabled two-factor authentication for improved security.

Our customers have the same options and it is up to our customers to implement security policies for their users.

Remote working

Access to our network and thereby potentially to systems and data is only possible for authorised individuals. Our employees have access via remote workplaces using VPN to RDS. Two-factor authentication is always used in cases of connection from an external location

Human resource security

Screening

We have procedures in place governing recruitment of employees and collaboration with externals ensuring that we recruit the right candidate based on background and skills. We have descriptions of roles and responsibilities for employees and employee categories to ensure that all employees are aware of their responsibilities. When joining the company, all employees are reviewed, and a registration form is followed.

Terms and conditions of employment

General terms of employment, including confidentiality regarding internal and customer matters, are described in each employee's employment contract where terms of all areas of the employment, including termination and sanctions in case of potential security breaches, are laid down.

During employment

Management responsibilities

In connection with employment, the new employee signs a contract. The contract states that the employee must observe the current policies and procedures. Moreover, it is clearly defined as part of the contract material what the employee's responsibilities and role comprise.

Information security awareness, education and training

Our assets are to a large extent our employees and we follow a structured set of methods in relation to our employees' qualifications, education and certifications. Courses, seminars and other relevant activities are organized on an ongoing basis, as a minimum once a year, to ensure that relevant employees and any external collaborating partners are kept up to date with security and are made aware of new threats, if any. Employees, and external partners where relevant to include them in our security guidelines, are periodically informed about our security guidelines and when amendments are made to them.

Disciplinary process

General terms of employment, including confidentiality about own and customer relationships, are described in each employee's employment contract, in which matters relating to all aspects of the employment, including termination and penalties in case of security breaches, are specified.

Termination or change of employment responsibilities

In the event of termination of employment, we have a thorough procedure which must be observed to ensure that the employees return all relevant assets, including portable media, etc. and to ensure that all employees' access to buildings, systems and data are revoked. The overall responsibility for securing the performance of all controls related to the termination process lies with the company's COO.

Asset Management

Asset inventory

Software, servers, and network devices, including configuration, are registered for use of documentation, overview of devices, etc. We have a complex network including many systems and customers and to prevent unauthorized access and to ensure a transparent structure, we have prepared documentation describing the internal network with devices, naming of devices, logical segmentation of networks, etc.

The documents and similar are regularly updated in the event of changes and are reviewed at least once a year by our network specialists.

Ownership of assets

By means of allocation of responsibilities and role descriptions central network devices, servers, peripherals, systems, and data are dedicated to system administrators in our company. Customer data and systems are dedicated to the customer's contact person.

Acceptable use of assets

This is described in the employee manual.

Return of assets

In the event of termination of employment, we have a comprehensive procedure in place which must be observed to ensure that the employees return all relevant assets, including portable media, etc., and to ensure that all employees' access to buildings, systems and data are revoked. The overall responsibility for all controls related to the termination process lies with the company's COO.

Management of removable media

We ensure to the widest extent possible that our staff's portable media, e.g. laptops, mobile phones and similar, are securely configured to the same extent as the rest of our environment; and we also ensure that the data carrying media are updated when we introduce new security measures.

Access management

Access control policy

We have a policy regarding the allocation of access. This policy is an integral part of our IT security policies.

User access management

User account creation and termination procedures

Our customers' users are only created upon request from our customers. Our customers are thereby responsible for the creation and termination of user accounts. For special deliveries to our customers, we have systems that automatically create users and provides the information needed for these.

All users must be personally identifiable, i.e. have a clear identification with a personal name. In case of service users, i.e. accounts only used for system purposes, the option regarding actual logon is disabled.

Allocation of rights

Allocation of privileges is controlled in connection with our normal user management process.

Management of secret authentication information of users

All personal logons are only known by the individual employee and are subject to password policies to ensure complexity.

Review of user access rights

Every month, the company's internal systems of users and their access levels are being evaluated to prevent unauthorized access. The overall responsibility of this lies with the company's COO.

User responsibilities

Use of secret authentication information

According to our IT security policies, our employees' passwords are personal. When changes are made in the internal information security policy, all employees are informed, ensuring that everybody is familiar with the latest update. Our internal policies are easily accessible to everybody. As we have users, such as service accounts and similar, that cannot be used for logon and for system-related reasons do not change passwords, we have a system for storage of such passwords. Only authorised staff has access to the system.

System and data access control

Information access restriction

Our employees are set up with differentiated access privileges and therefore only have access to the systems and data that are relevant for their work effort.

Password management system

All employees across both customer systems and proprietary systems have restrictions as regards passwords. All users have a password and systemically it is set up in such a way that there are restrictions in relation to the design of the password.

Our IT security policy describes rules for complexity and that our employees' passwords are personal, and only the user may know the password.

Physical and environmental security

Equipment maintenance

The data center's cooling and fire prevention systems are checked regularly and the back-up power system (diesel generators & UPS) is checked every six months. Systems are installed in the data center monitoring temperatures and voltages in the server room.

Securing equipment and assets off-premises

We conduct back-up procedures during the night to protect our customers' data and systems in case our hosting systems for some reason become unavailable.

We have entered into an agreement with the concerned supplier on housing of our proprietary servers and similar measures are implemented to protect against theft, fire, water, and temperature deviations.

We annually receive an auditor's assurance report covering the physical security at our sub-suppliers.

Most recently we have received auditor's assurance report covering the period 01-01-2018 to 31-12-2018. The report has been issued subject to reservations. A risk analysis has been performed, covering these reservations, and further changes have not been considered necessary.

Secure disposal or re-use of equipment

All data-carrying devices are destroyed before disposal to ensure that no data is accessible.

Unattended user equipment

All internal user accounts are centrally managed to enter screen lock mode after a maximum of 2 minutes of inactivity. Thereby we ensure that unauthorized staff cannot access confidential data.

Operations security

Documented operating procedures

Although our organization does not necessarily allow overlap within all projects and systems, we ensure via documentation and descriptions - and via competent and diligent employees - that existing or new employees can commence working on a system for which the said person does not have operational or previous experience. We operate with dual roles on all systems to ensure that the key responsible employee is responsible for communicating practical issues to their colleagues. The system documentation is updated continuously.

Change management

We have defined a process for change management to ensure that changes are made as agreed with customers and are properly planned according to the in-house conditions. Changes are only made based on a qualification of the project, the complexity and assessment of effects on other systems. Moreover, a process is followed regarding development and testing.

At all internal changes in vital operating components, we always ensure as a minimum that:

- All changes are discussed, prioritized and approved by management
- All changes are tested
- All changes are approved prior to deployment
- All changes are deployed at a specified time in agreement with the company and customers
- Fall-back planning is performed, ensuring that the changes can be rolled back or cancelled in case they fail to be operational
- The system documentation is updated according to the new change in case it is found necessary.

At standard changes a risk assessment is not needed, and similarly, management approval is not necessary. However, all standard changes require the customer's written approval.

Our environment is logically segregated and divided into testing and production whereby we ensure that a product is tested before it is brought into production. By means of access controls we ensure that only authorised personnel have access to this.

Capacity management

Via our general monitoring system, we have set limits for when our overall systems, and thereby our customers' systems, must be upscaled regarding electronic space, response time, etc. When we set up new systems, functionality testing must be performed, including capacity and performance testing. A regular procedure has been prepared for reporting capacity issues.

Protection against malware and DDoS

Controls against malware and DDoS

We have implemented scanning and monitoring systems to protect against known harmful code, i.e. what we and our customers - via our platforms - may risk being infected with on the Internet via mails etc. We have antivirus systems, anti-malware on all platforms, systems for monitoring Internet usage, traffic and resources on SaaS platforms, security in other technical and central installations (firewall etc.) in place. Additionally, we provide anti-DDoS solutions for securing against DDoS attacks.

We continually improve protection against new cryptoware variants to ensure that our data and systems are protected against known cryptoware variants.

Backup

Information backup

We ensure that we can restore systems and data appropriately and correctly, and in compliance with the agreements we have with our customers.

We have a test for how systems and data can be restored in practice. We keep a log of these tests, enabling us to follow up on whether we can change our procedures and processes to improve our solution.

Unless otherwise agreed with our customers, we perform backup of their entire virtual environment with us. We perform backups of our proprietary systems and data in the same manner as when we perform backups of customers' systems and data.

We have defined guidelines as to how we perform backups. Every night a complete copy of our central system is transferred to our backup systems. Thereby the data is physically separated from our operational systems, and after completion an automatic verification is performed to check if the amount and content of data between our operational system and backup system match.

A responsible employee will then ensure that the backup is completed and will take the necessary action if the job has failed, and afterwards enter it in the log.

Logging and monitoring

Event logging

We have set up monitoring and logging of network traffic, and our operations department follows this. We do not perform proactive monitoring of logged incidents, but we follow up if we suspect that an incident can be related to issues addressed in the log. For management of monitoring and follow-up on incidents we have implemented formal incident and problem management procedures to safeguard that incidents are

registered, prioritized, managed, escalated and that necessary actions are taken. The process is documented in our hotline system.

Protection of log information

Logs are uploaded to our log server.

Administrator and operator log

Administrator logs occur simultaneously with the normal log.

Time synchronization

We use NTP servers from the Internet, which all servers are synchronized up against.

Managing software on operating systems

Via our patch process, we ensure that only approved and tested updates are installed. We ensure that critical patches, affecting security are never installed later than 2 months after they are released. In the event of major changes, this well be discussed at internal meetings in the operations department.

Moreover, our staff is aware of the policy regarding download of software.

Management of technical vulnerabilities

Security announcements from DK-CERT are monitored and analyzed and if they are found relevant, they are installed on our internal systems within 1 month from release. Additionally, we regularly perform a risk assessment of our in-house solutions.

Communications security

Network controls

The IT security procedures regarding the external framework for systems and data are the network against the Internet, remote or similar. Protection of data and systems within the network and external protection against unauthorized access is of the highest priority to us. All cabling internally and to/from our systems is redundant along the entire stretch.

Securing network services

Our customers have access to our systems either via the public networks, where access is allowed via encrypted VPN access, or MPLS. Access and communication between our servers and our co-location takes place within a closed network.

Only approved network traffic (inbound) is allowed through our firewall.

We are responsible for operations and security with us, i.e. from our systems onwards and out to the Internet (or MPLS). Our customers are responsible for being able to access to the Internet.

Segregation of networks

Our network is divided into several segments whereby we ensure that our internal network is segregated from the customers' networks. Moreover, the services containing sensitive data are placed in specially secured environments.

Policies and procedures for data transfer

External data communication only takes place via mails, as our customers' access to and use of our servers are not considered external data communication.

Initial temporary passwords to customer systems are sent via mail, but they must be changed at first logon. Forgotten passwords, personal information, orders, etc. are never handled via phone, but only in writing and not until our staff has verified that it is a real and authorised person that we are communicating with.

Confidentiality agreements

We have established confidentiality in general for all parties involved in our business. This is done by means of employment contracts or service agreements with sub-suppliers and business partners.

System acquisition, development and maintenance

Information security requirements analysis and specification

If a new system is introduced, analyses and research will be carried out to ensure that it complies with best practice for hardening.

Change management procedures

We have defined a process for change management to ensure that changes are made as agreed with customers and are properly planned according to the in-house conditions. Changes are only made based on a qualification of the project, the complexity and assessment of effects on other systems. Moreover, a process is followed regarding development and testing, as well as acceptance by us and the customer.

In case of fundamental changes to the underlying systems operating our environment, we always ensure as a minimum that:

- All changes are discussed, prioritized and approved by management
- All changes are tested
- All changes are approved before deployment
- All changes are deployed at a specific time as agreed with the business and any customers
- Fall-back planning is performed, ensuring that the changes can be rolled back or cancelled in case they fail to be operational
- The system documentation is updated with the new change in case it is found necessary.

In case of a “standard change” – that is, a change that can be approved without test cycle or risk assessment, the customer’s written approval must always be obtained before the change is performed.

Our environment is logically segregated and divided into testing and production, whereby we ensure that a product is tested before it is brought into production. By means of access controls we ensure that only authorised personnel have access hereto.

Restriction on changes to software packages

Service packs and system specific updates that may cause changes to functionality are reviewed and installed separately. Security updates are rolled out on all systems insofar it is possible.

Supplier relationships

Management of changes to services

When changes occur internally in the organization, including policies and procedures, and changes are made to our services or services from our external partners, a risk assessment will always be performed to explore whether the changes will have an impact on our agreement with the customers.

Monitoring of third-party services

Via monitoring set up by a third party we ensure that all services delivered by third parties are in compliance with the requirements and terms we have agreed with third parties. We regularly visit third parties, whereby we ensure that the agreed terms are continually complied with.

Information security incident management

Responsibilities and procedures

Our employees are under obligation to keep themselves updated by means of providers' support sites, discussion forums etc. regarding known weaknesses in the systems we use and provide.

There are formally appointed ASPs and the requirements they are subject to are clearly and formally defined. The ASPs are responsible for preparing and maintaining procedures that ensure timely and correct intervention in connection with security breaches.

Reporting of information security breaches

Our hotline system that we use for handling all issues for customers and internal matters is the same system that we use to handle security incidents. Here we can escalate issues in such a manner that some incidents have higher priority than others. Furthermore, security incidents identified from own observations, alerts from log and monitoring systems, telephone calls from customers, sub-suppliers or partners, respectively, are escalated from our hotline to the operations department, alerting management as well.

We have established contact to a hotline at DK-CERT with whom we have entered into a mutual agreement on notification in case of significant security related matters regarding Internet traffic.

Reporting security weaknesses

Our employees and external partners are, via the entered contracts and agreements, under an obligation to report any security incident to their immediate superior to ensure that action can be taken to address the issue as soon as possible and that necessary measures can be taken in accordance with the established procedures.

Business continuity management

Information security continuity

In the event of an emergency, any.cloud has prepared a business continuity plan. The business continuity plan is embedded in the IT risk analysis and is updated at least once a year in continuation of the conduction of the analysis.

The plan and the procedures are embedded in our operations documentation and procedures.

We ensure that this is done by having considered the risks, classified the units in our operations, and having procedures in place that ensure that we in our business continuity planning can perform replacement of our operations platform to ensure that the services supplied will be restored in a timely manner.

Testing, maintenance and reassessment of business continuity plans

The plan is tested as a dry run, once a year, as part of our business continuity procedure for us to ensure that the customers to the smallest extent possible will experience interruption of services in connection with any emergency.

Compliance

Independent review of information security

A review is performed by an external IT auditor as well as in connection with the preparation of the annual ISAE 3402 reports.

Compliance with security policies and standards

Our employees read the IT security policies once a year as a minimum. We have on-going controls, performed by our management team, to ensure that our employees comply with the security measures specified in our IT security policies, this is applicable for the physical as well as the logical conditions.

Technical compliance review

We have established procedures that ensure that all systems are updated, and we have implemented extensive monitoring of all systems, including our customers' services. Moreover, we have, with another ISO certified hosting provider, an external system monitoring the availability of all our services. Furthermore, we have controls ensuring compliance with monitoring and security.

Changes in the period

Throughout the period from 20 March 2020, very few significant changes have occurred. We have increased the competency of our technical staff in terms of new appointments, and furthermore we have:

- Improved our system for documenting tasks
- Implemented and documented new products
- Developed and improved internal systems.

Supplementary controls

any.cloud A/S' customers are, unless otherwise agreed, responsible for establishing a connection to any.cloud A/S' servers. Furthermore, any.cloud's customers are, unless otherwise agreed, responsible for:

- Ensuring that the agreed backup level meets the customer's needs
- Periodically reviewing the customer's own users and system resources
- Compliance with any.cloud A/S' at any time applicable Service Level Agreement, which can be found on any.cloud A/S' website
- Maintaining traceability in third-party software, managed by the customer.

Section 3: Independent service auditor's assurance report on the description of controls, their design and functionality

To the management of any.cloud, their customers, and their auditors.

Scope

We have been engaged to report on any.cloud A/S' description presented in Section 2. The description covers any.cloud A/S' operating and hosting services in the period 01-12-2018 to 30-11-2019, as well as the design and operation of the controls related to the control objectives, stated in the description.

any.cloud A/S' responsibility

any.cloud A/S is responsible for preparing the description (section 2) and the related statement (section 1) including the completeness, accuracy and method of presentation of the description and statement. Additionally, any.cloud A/S is responsible for providing the services covered by the description, and for the design, implementation and effectiveness of operating controls for achieving the stated control objectives.

REVI-IT A/S' independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behavior.

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

REVI-IT A/S' responsibility

Based on our procedures, our responsibility is to express an opinion on any.cloud A/S' description (section 2) as well as on the design and functionality of the controls related to the controls objectives stated in this description. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organization", issued by IAASB. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organization, described in section 2.

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 organization

any.cloud A/S' description in section 2 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 systems that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion is formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in any.cloud A/S' description in Section 2 and on the basis of this, it is our opinion that:

(a) the description of the controls, as they were designed and implemented, throughout the period 01-12-2018 to 30-11-2019, is fair in all material respects
(b) the controls related to the control objectives stated in the description were suitably designed throughout the period from 01-12-2018 to 30-11-2019 in all material respects
(c) the controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 01-12-2018 to 30-11-2019.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these are listed in the subsequent main section. (Section 4)

Intended users and purpose

This assurance report and the description of test controls in section 2 - is intended only for customers who have used any.cloud A/S' hosting services and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves, when evaluating the risks of significant misinformation in the financial statements.

Copenhagen,

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State Authorised Public Accountant

Basel Obari
It-auditor (CISA, CISM), Director, Partner

Section 4: Control objectives, controls, tests, and related test controls

The following overview is provided to facilitate an understanding of the effectiveness of the controls implemented by any.cloud A/S. Our testing of functionality comprised the controls that we considered necessary to provide reasonable assurance that the control objectives stated in the description were achieved during the period 01-12-2018 to 30-11-2019

Thus, we have not necessarily tested all the controls mentioned by any.cloud A/S in the description in Section 2.

Moreover, our statement does not apply to any controls performed at any.cloud A/S' customers, as the customers' own auditors should perform this review and assessment.

We performed our tests of controls at any.cloud A/S by taking the following actions:

Method	General description
Enquiry	Interview, i.e. enquiry with selected personnel at the company regarding controls
Observation	Observing how controls are performed
Inspection	Review and evaluation of policies, procedures, and documentation concerning the performance of controls
Re-performing control procedures	We have re-performed – or have observed the re-performance of – controls in order to verify that the control is working as assumed

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

Risk Assessment and management

Risk assessment

Control objective: to ensure that the company periodically performs an analysis and assessment of the IT risk profile.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
4.1	We have procedures in place for ongoing risk assessment of our business, especially our cloud services. That way, we ensure that the risks related to our provided services are minimized to an acceptable level. Risk assessment is performed periodically and when we introduce changes or implement new systems that we deem relevant in relation to re-performing our general risk assessment. The responsibility of risk assessments is embedded with the company's CTO and subsequently approved by management.	We have inquired about the preparation of a risk analysis, and we have inspected the prepared risk analysis. We have inquired about review of the risk analysis during the period, and we have inspected documentation for the risk analysis being reviewed and approved by management during the audit period.	No significant deviations noted.

Information security policies

Management direction for information security

Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

Nr.	any.cloud A/S' control	REVI-IT's test	Test results
5.1	We have defined our quality control system based on our overall objective to deliver stable and secure hosting to our customers. To do that, it has been necessary to introduce policies and procedures, ensuring that our services are homogenous and transparent. Our IT security policy is prepared with reference to the above and is valid for all employees and all deliverables. We are ISO 27001 certified and we continuously improve our policies, procedures, operations as well as physical and logistic security.	We have inquired about the preparation of an information security policy, and we have inspected the document. We have inquired about periodic review of the information security policy, and we have checked that the document has been reviewed during the audit period. Additionally, we have inspected the control for periodic review of the document. We have inquired about management approval of the information security policy, and we have inspected documentation for management approval.	No significant deviations noted.

Organization of information security

Internal organization

Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
6.1	We have a clearly defined organization in regard to delegation of responsibilities; and we have comprehensive descriptions of responsibilities and roles at all levels, from management to each individual operations employee. Confidentiality has been established with all involved parties. This is ensured by employment contracts and non-disclosure agreements. Through continuous documentation and processes we ensure that we can eliminate or minimize key staff dependency. We have established contact to a hotline at DK-CERT. We assess whether projects comply with our information security or not. If not, the project will either be adjusted or discarded.	We have inquired about allocation of responsibility for information security, and we have inspected documentation for the allocation and maintenance of descriptions of responsibilities. We have inquired about access segregation in relation to function, and we have inspected documentation for differentiated access. We have inquired about contact with interest groups, and we have inspected documentation for contact. We have inquired about the consideration of information security in project management. We have in spot checks inspected projects and verified that information security is considered.	No significant deviations noted.

Mobile devices and teleworking

Control objective: to ensure the security of teleworking and use of mobile devices.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
6.2	We have implemented the possibility for both our employees and our customers to use mobile devices (smartphones, tablets e.g.) Besides password protection, we have two-factor authentication for improved security. Access to our network and potentially systems and data, is only possible for authorised individuals. Our employees have access via remote workplaces using VPN. Two-factor security is always used when the system is accessed from outside.	We have inquired about mobile device management, and we have inspected the solution. We have inquired about securing remote workplaces, and we have inspected the solution.	No significant deviations noted.

Human resource security

Prior to employment

Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
7.1	We have descriptions of roles and responsibilities for employees and employee categories to ensure that all employees are aware of their responsibilities.	We have inquired about a procedure for hiring new employees, and we have inspected the procedure. Additionally, we have in spot checks inspected documentation for the procedure being followed. We have inquired about the formalization of terms of employment, and we have in spot checks inspected the contents of contracts.	No significant deviations noted.

During employment

Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
7.2	The contract states that the employee must observe the current policies and procedures. Moreover, it is clearly defined as part of the contract material what the employee's responsibilities and role comprise. Courses, seminars and other relevant activities are organized on an ongoing basis, as a minimum once a year, to ensure that relevant employees are kept up to date with security and are made aware of new threats, if any. General terms of employment, including non-disclosure agreements about company and customer information, are described in every contract, where all aspects of employment, termination of employment and sanctions connected with security incidents are stated.	We have inquired about management's responsibility for communicating policies and procedures, and we have inspected documentation for the allocation of responsibility. We have inquired about further staff training, and we have in spot checks inspected documentation for further training. We have inquired about guidelines for disciplinary processes, and we have inspected the guidelines.	No significant deviations noted.

Termination and change of employment **Control objective: To protect the organization's interests as part of the process of changing or terminating employment.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
7.3	In the event of termination of employment, we have a thorough procedure which must be observed to ensure that the employees return all relevant assets, including portable media, etc. and to ensure that all employees' access to buildings, systems and data are revoked.	We have inquired about employees' obligations to maintaining information security in connection with termination of employment, and we have inspected documentation for the employees' obligations.	No significant deviations noted.

Asset management

Responsibility for assets **Control objective: To identify organizational assets and define appropriate protection responsibilities.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
8.1	Through assignment of responsibilities and role descriptions, the central network, servers, remote units, systems and data allocated to application service provider in our company. Data and systems belonging to the customer are allocated to the customer contact person. The management of assets are described on the employee handbook. Upon termination of employment, we have a comprehensive procedure in place to ensure that the employees return all relevant assets, including portable media and securing that all access to buildings, systems and date are discontinued.	We have inquired about inventories of assets, and we have in spot checks inspected inventories of assets. We have inquired about an inventory of asset ownership, and we have inspected the inventory. We have inquired about guidelines for the use of assets, and we have inspected the guidelines. We have inquired about a procedure for ensuring the return of handed-out assets, and we have in spot checks inspected the procedure.	No significant deviations noted.

Information classification **Control objective. To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
8.2	By means of allocation of responsibilities and role descriptions central network devices, servers, peripherals, systems, and data are dedicated to system administrators in our company. Customer data and systems are dedicated to the customer's contact person.	We have inquired about a policy for information classification, and we have inspected the policy. We have inquired about the labelling of data, and we have inspected the guidelines for labelling data. We have inquired about guidelines for handling assets, and we have inspected the guidelines.	No significant deviations noted.

Media handling Control objective: To prevent disclosure, modification, removal or destruction of information stored on media.			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
8.3	We ensure that our staff's media, e.g. laptops, mobile phones and similar, are securely configured to the same extent as the rest of our environment, and that we make sure that data-bearing media are updated, when we implement new security precautions.	We have inquired about mobile device management, and we have inspected documentation for the solution. We have inquired about guidelines for the disposal of media. We have inquired about transport of portable media.	Since the company reports, that they have not had any disposals of data during the period, we have not tested for disposal of media. No significant deviations noted.

Access control

Business requirements of access control Control objective: To limit access to information and information processing facilities.			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
9.1	We have a policy regarding the allocation of access. This policy is an integral part of our IT security policies.	We have inquired about a policy for management of access to systems and buildings, and we have inspected the policy. We have inquired about management of access to network and network services, and we have inspected the solution.	No significant deviations noted.

User access management **Control objective: To ensure authorised user access and to prevent unauthorized access to systems and services.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
9.2	Our customers' users are only created upon request from our customers. Our customers are thereby responsible for the creation and termination of user accounts. Upon special deliveries to our customers, we have systems that automatically creates users and delivers the information about these. All uses must be personally identifiable, i.e. have a clear identification with a personal name. Allocation of privileges is controlled in connection with our normal user management process. All personal logons are only known by the individual employee and are subject to password policies to ensure complexity. Every month the company's in-house systems for creation of users and their access level, are reviewed to prevent unauthorized access.	We have inquired about a procedure for creating and disabling users, and we have inspected the procedures. We have inquired about a procedure for allocating rights, and we have inspected the procedure. We have inquired about monitoring of the use of privileged access rights, and we have in spot checks inspected documentation for monitoring. We have inquired about storage of confidential passwords, and we have inspected documentation for adequate storage. We have inquired about a process for periodic review of users, and we have inspected documentation for the latest review. We have inspected the procedure for revocation of rights.	No significant procedures noted.

User responsibilities **Control objective: To make users accountable for safeguarding their authentication information.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
9.3	According to our IT security policies, our employees' passwords are personal. Whenever internal information security changes, all employees are informed, so they are always familiar with the latest version. Our internal policies are accessible to all our staff.	We have inquired about guidelines for the use of confidential passwords, and we have inspected the guidelines.	No significant guidelines noted.

System and application access control **Control objective: To prevent unauthorized access to systems and applications.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
9.4	Our employees are set up with differentiated access privileges and therefor only have access to the systems and data that are relevant for their work effort. As we have users like service accounts and similar, that cannot be used for login, and due to system related issues don't change passwords, we have a system for storing these specific passwords. Only authorised staff has access to the system.	We have inquired about restrictions on access to data, and we have inspected documentation for restriction. We have inquired about a procedure for secure logon, and we have inspected the solution. We have inquired about a system for password management.	No significant deviations noted.

Cryptography

Cryptographic controls **Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
10.1	The security policy describes requirements to cryptography	We have inquired about a policy for the use of encryption, and we have in spot checks inspected the use of cryptography.	No significant deviations noted.

Physical and environmental security

Secure areas

Control objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
11.1	The cooling and fire protection system is periodically inspected. The backup power system (Diesel generators and UPSs) are inspected every 6 months. The datacenter has systems monitoring temperatures and voltage in the server room. Every night we run backup procedure to ensure our customer's data and systems, in case our hosting systems should accidentally be inaccessible for one reason or another. Furthermore, we transfer a copy to our remote datacenter. Yearly we receive auditor's assurance report describing adequate physical security with our sub-suppliers.	We have inquired about an auditor's assurance report from the sub-supplier of the physical environment, and we have inspected the auditor's assurance report for adequate physical security. We have inquired about the allocation and revocation of access to operations facilities at the sub-supplier, and we have in spot checks inspected documentation for the allocation of access to operations facilities. We have inspected the physical environment at the company's offices to check the physical security We have inquired about deliverance of parcels and goods.	We have observed deviations in sup-supplier's assurance report: In sup-supplier's assurance report, it is stated that deviations from procedure regarding approval of employee's physical access to secure areas, have been found. A significant part of the spot tests has shown deviations. It has been stated that corrective actions have been implemented as of 30.04.2019. No further deviations noted.

Equipment

Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
11.2	We have an agreement with the sup-supplier in question about housing of our own servers, and a similar system to prevent theft, fire, water and deviations in temperature has been implemented. We receive yearly auditor's assurance reports, uncovering the physical safety with our sub-suppliers. All data-carrying devices are destroyed before disposal, so ensure that no data is accessible. All internal user accounts are centrally managed to enter screen lock mode, after a maximum of 2 minutes of inactivity. Hereby we secure that unauthorized personnel won't get access to confidential data.	We have inquired about an auditor's opinion from sub-supplier regarding physical environment, including the securing of cabling, disposal of equipment and portable storage. We have inspected the auditor's opinion from sub-supplier to identify supporting supplies and to ensure regular maintenance of the equipment. We have inquired about periodic inspection of external location and have as a spot check inspected the documentation for inspection. We have inquired about securing of unattended user equipment and performed spot check to make sure that user equipment is locked when inactive. We have inquired into policy for clean desk.	No significant deviations noted.

Operations security

Operations procedures and responsibilities

Control objective: To ensure correct and secure operation of information processing facilities.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
12.1	We operate with dual roles on all systems to ensure that the key responsible employee is responsible for communicating practical issues to their colleagues. The system documentation is updated continuously. Changes are only made based on a qualification of the project, the complexity and assessment of effects on other systems. Moreover, a process is followed regarding development and testing. When we set up new systems, functionality testing must be performed, including capacity and performance testing.	We have inquired about procedures in connection with operations, and we have in spot checks inspected the procedures. We have inquired about change management, and we have in spot checks inspected documentation for change management during the period. We have inquired about capacity monitoring, and we have in spot checks inspected documentation for capacity monitoring. We have inquired about the use of a test environment, and we have inspected documentation for the existence of a test environment.	No significant deviations noted.

Protection from malware

Control objective: To ensure that information and information processing facilities are protected against malware.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
12.2	We have antivirus systems, anti-malware on all platforms, systems for monitoring Internet usage, traffic and resources on SaaS platforms, security in other technical and central installations (firewall etc.) in place.	We have inquired about measures to protect against malware. We have inquired about the use of antivirus software, and we have inspected documentation for the use.	No significant deviations noted.

Backup

Control objective: To protect against loss of data.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
12.3	We have defined guidelines as to how we perform backups. Every night a complete copy of our central system is transferred to our backup systems. Thereby the data is physically separated from our operational systems and after completion an automatic verification is performed to check if the amount and content of data between our operational system and backup match.	We have inquired about the configuration of backup, and we have in spot checks inspected documentation for the setup. We have inquired about the storage of backup, and we have inspected the auditor's assurance report from sub-supplier in order to verify that backup is stored securely. We have inquired about test of restore from backup files, and we have inspected documentation for restore test.	No significant deviations noted.

Logging and monitoring **Control objective: To record events and generate evidence.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
12.4	We have set up monitoring and logging of network traffic, and our operations department follows this. We do not perform proactive monitoring of logged incidents, but we follow up if we suspect that an incident can be related to issues addressed in the log. For management of monitoring and follow-up on incidents we have implemented formal incident and problem management procedures to safeguard that incidents are registered, prioritized, managed, escalated and that necessary actions are taken. Logs are uploaded to our log server. Administrator logs occur simultaneously with the normal log. We use NTP servers from the Internet, which all servers are synchronized up against.	We have inquired about the logging of user activity. We have in spot checks inspected the logging configurations. We have inquired about the securing of log information, and we have inspected the solution. We have inquired about synchronization with an adequate clock server, and we have inspected the solution.	No significant deviations noted.

Control of operational software **Control objective: To ensure the integrity of operational systems .**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
12.5	By means of our patch process we ensure that critical patches that have an effect on security are installed no later than 2 months after they are released. In the event of major changes, this will be discussed at internal meetings in the operations department.	We have inquired about guidelines for installation of software on operations systems, and we have inspected the guidelines. We have inquired about timely updates to operations systems, and we have inspected documentation for updates of operations systems.	No significant deviations noted.

Technical vulnerability management **Control objective: To prevent exploitation of technical vulnerabilities.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
12.6	Security announcements from DK-CERT are monitored and analyzed and if they are found relevant, they are installed on our internal systems within 1 month from release. Additionally, we regularly perform a risk assessment of our in-house solutions. In addition, our employees are familiar with the policy regarding download of software.	We have inquired about technical vulnerability management, and we have inspected documentation for this management. We have inquired about management of access to installing software, and we have inspected documentation for the limitation of users with rights allowing them to install software.	No significant deviations noted.

Communications security

Network security management **Control objective: To ensure the protection of information in networks and its supporting information processing facilities.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
13.1	Protection of data and systems within the network and external protection against unauthorized access is of the highest priority to us. All cabling internally and to/from our systems is redundant along the entire stretch. Our customers have access to our systems either via the public networks, where access is allowed via encrypted VPN access, or MPLS. Access and communication between our servers and our co-location takes place within a closed network. Our network is divided into several segments whereby we ensure that our internal network is segregated from the customers' networks.	We have inquired about measures to secure network and network services. We have inspected documentation for the establishment of firewall and patching of firewall. We have inquired about securing network services, and we have inspected documentation for adequate securing.	No significant deviations noted.

Information transfer **Control objective: To maintain the security of information transferred within an organization and with any external entity.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
13.2	External data communication only takes place via mails, as our customers' access to and use of our servers are not considered external data communication. Initial temporary accessing customer systems are sent by encrypted mail and must be changed at first logon. We have established confidentiality in general for all parties involved in our business. This is done by means of employment contracts or service agreements with sub-suppliers and business partners.	We have inquired about policies and procedures for data transfer. We have inquired about agreements regarding data transfer. We have inquired about guidelines for transmitting confidential information. We have inquired about the establishment of confidentiality agreements, and we have inspected documentation for the establishment.	No significant deviations noted.

Supplier relationships

Information security in supplier relationships **Control objective: To ensure protection of the organization's assets that are accessible by suppliers.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
15.1	When changes occur internally in the organization, including policies and procedures, and changes are made to our services or services from our external partners, a risk assessment will always be performed to explore whether the changes will have an impact on our agreement with the customers.	We have inquired about the formalization of supplier agreements, and we have inspected the agreement in order to check the consideration of information security. We have inspected an auditor's assurance report from sub-supplier in order to identify whether there are any significant observations in relation to the company's agreement with the sub-supplier.	No significant deviations noted.

Supplier service delivery management **Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.**			
Nr.	any.cloud A/S' control	REVI-IT's test	Test result
15.2	Whenever changes are made within the organization, including policies and procedures, together with changes in our services or services from external partners, a risk assessment is always performed to encounter whether the change will affect our agreement with the customer.	We have inquired about monitoring of supplier services, and we have inspected documentation for monitoring. We have inquired about a policy for change management at sub-suppliers.	We have observed that the company is not able to document that it in a timely manner has considered the relevance or consequence of the findings the supplier's auditors have made in in their assurance report for sub suppliers reports, in relation to the company's service delivery. We have; however, inspected that the control has been performed and that relevant observations are documenter after end of period. No further deviations noted.

Information security incident management

Management of information security incidents and improvements

Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
16.1	ASP has formally been appointed and the requirements have been clearly and formally defined. The ASPs are responsible for preparing and maintaining procedures that ensure timely and correct intervention in connection with security breaches. Our hotline system that we use for handling all issues for customers and internal matters is the same system that we use to handle security incidents. Moreover, security incidents identified from own observations, alerts from log and monitoring systems, telephone calls from customers, sub-suppliers or partners, respectively, are escalated from our hotline to the operations department, alerting management as well. Our employees are, under an obligation to report any security incident to their immediate superior to ensure that action can be taken to address the issue as soon as possible and that necessary measures can be taken in accordance with the established procedures.	We have inquired about responsibility and procedures in case of information security incidents, and we have inspected documentation for the allocation of responsibilities. Additionally, we have inspected the procedure for managing information security incidents. We have inquired about guidelines for reporting information security incidents and weaknesses, and we have inspected the procedure. We have inquired about information security incidents during the period. We have inquired about a procedure for assessment, reaction, and evaluation of information security incidents, and we have inspected the procedure.	It hasn't been possible to test information security incident management, since the company informs, that they have not experienced any security incidents during the period. No significant deviations noted.

Information security aspects of business continuity management

Information security continuity

Control objective: Information security continuity should be embedded in the organization's business continuity management systems.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
17.1	The business continuity plan is embedded in the IT risk analysis and is updated at least once a year in continuation of the conduction of the analysis.	We have inquired about the preparation of a business continuity plan for securing the continuity of operations in case of failures and similar, and we have inspected the plan. We have inquired about the implementation of compensating measures in connection with testing the business continuity plan, and we have inspected documentation for the implementation. We have inquired about test of the business continuity plan, and we have inspected documentation for completed test. Additionally, we have inquired about reassessment of the business continuity plan, and we have inspected documentation for the reassessment.	No significant deviations noted.

Redundancies

Control objective: To ensure availability of information processing facilities.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
17.2	The plan is dry tested once a year as part of our business continuity procedure for us to ensure that the customers to the smallest extent possible will experience interruption of services in connection with any emergencies.	We have inquired about the availability of operations systems, and we have inspected the established measures.	No significant deviations noted.

Compliance

Information security reviews

Control objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.

Nr.	any.cloud A/S' control	REVI-IT's test	Test result
18.2	We have established procedures that ensure that all systems are updated, and we have implemented extensive monitoring of all systems, including our customers' services. Moreover, we have, with another ISO certified hosting provider, an external system monitoring the availability of all our services. Furthermore, we have controls ensuring compliance with monitoring and security.	We have inquired about independent evaluation of the information security. We have inquired about internal controls for ensuring compliance with security policy and procedures, and we have inspected selected controls. We have inquired about periodic control of technical compliance, and we have inspected documentation for monitoring.	No significant deviations noted.