REVI·IT
IT-REVISION & RÅDGIVNING

Independent service auditor's assurance report on the description of controls, their design and operating effectiveness regarding the operation of hosted services for the period 01-12-2015 to 30-11-2016

ISAE 3402-II

any.cloud A/S

CVR-no.: 31 16 15 09

December 2016

This report was originally prepared in Danish.

In case of any disputes, the report in Danish is applicable.

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 01-12-2015 to 30-11-2016. 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
- 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 objectives
- 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 organisation's system throughout the period 01-12-2015 to 30-11-2016

(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 01-12-2015 to 30-11-2016. 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 01-12-2015 to 30-11-2016.

Copenhagen, 19 December 2016

any.cloud A/S

Gregor Møller
CEO

Section 2: any.cloud A/S' description of controls in relation to the operation of 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 organisation, ISAE 3402.

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

The description includes the control areas and controls with any.cloud, which include the majority of our customers and are based on our standard delivery. Individual customer matters are not included in this description.

any.cloud A/S

any.cloud provides professional ISO-certified hosting- and consultancy services to the Danish business community.

any.cloud's most significant activity is supplying services, including:

- PaaS - VPS (Virtual Private Server)
- DRaaS - virtual backup with DRS (Disaster Recovery Solution)
- Network security
- MPLS and fibre infrastructure
- DDoS and hacking security products
- Consultancy, support and operations

We supply the highest quality of infrastructure through the best suppliers such as IBM and VMware and present this to our customers by means of simple and innovative solutions.

We make a great effort to render complicated services simple for our customers. We take over all the machines and systems usually whirring in a server room in order for the customer to focus on their business. We operate IT for companies and their employees and ensure that they always can work – securely, efficiently, and at a very favourable price.

any.cloud has an ISAE 3402 Type II assurance report and works under the ISO 27002 standard. This ensures that we constantly maintain the quality needed to belong to the absolute elite within hosted IT solutions.

any.cloud is hosted at InterXion Denmark in Ballerup and Global Connect in Taastrup; both are European suppliers of cloud and operator neutral data centres with more than 48 data centres in 11 countries. We provide all relevant security measures such as Inergen, cooling, redundant power sources, fibre lines, and fully equipped monitoring systems. Additionally, any.cloud has hosting services in the IBM-owned company Softlayer, who has 31 data centres, whereby any.cloud can supply their solutions worldwide.

Any.cloud is, i.a. due to our recertifications of the hosting certificate from BFIH, part of Denmark's best hosting companies. As a continually certified member and with the attainment of the hosting brand any.cloud is

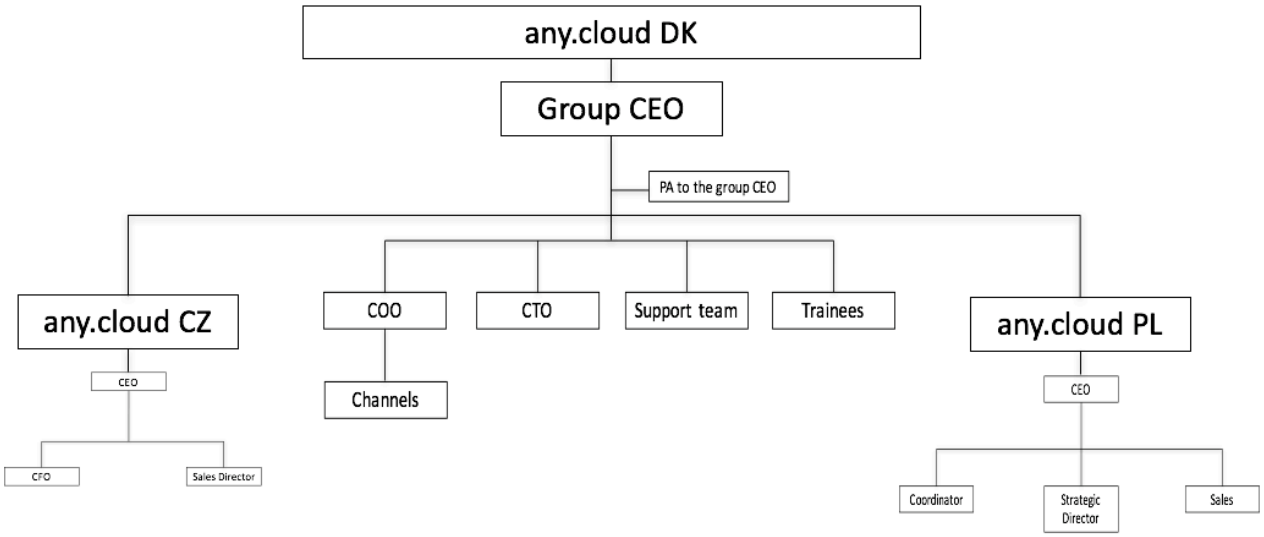
obliged to provide in consideration of strict control measures, high security requirements, and transparency in relation to the contents of quality and security in IT hosting services.

We are a strong, composed team with departments in Denmark, Poland and The Czech Republic.

any.cloud – RESHAPE THE FUTURE

Organisation and responsibilities

any.cloud has a clear and transparent corporate structure.



any.cloud A/S has 15 employees, covering the departments Administration, Finance, and Operations-Support. An additional 16 persons are employed in the sister company any.mac A/S providing all on-site support and operations for any.cloud's customers.

Thus, any.cloud's employees solely work on the hosting infrastructure.

Support receives all incoming inquiries and either solves the customer's issues or forwards the task to Operations for processing.

Operations thus functions both as second line support for hotline and additionally handles the practical implementation of new customers; monitors existing operations solutions and any other tasks in connection with the day-to-day management of our hosting environment.

Risk assessment and management

Risk assessment

IT risk analysis

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

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

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

Management of security risks

Procedure for risk management

We have introduced a scoring system with regard to the risks related to the provision of cloud services. We use the calculation formula risk*effect with a score from 1 to 10. The acceptable level is up to 30 points. It is continuously assessed whether we can reduce risks and take measures to improve our score.

Security policies

IT security policies

Policies for information security

We have defined our quality control system based on our overall objective to deliver stable and secure hosting to our customers. In order to do that, we have introduced policies and procedures ensuring that our deliveries are uniform and transparent.

Our IT security policy is prepared with reference to the above and applies to all employees and all our deliveries.

Our methods for implementation of controls are defined according to ISO 27002 (framework for management of information security) and is overall divided into the following control areas:

- Organisation and responsibilities
- Human resource security
- Logic access control
- Risk assessment and management
- Physical and environmental security
- Use of IT equipment
- Procedures for operations
- The network
- Support
- Protection against malware
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management.

We continuously improve our policies, procedures and operations.

We are a member of BFIH (Brancheforeningen for IT-Hostingvirksomheder i Danmark – Trade association for IT hosting companies in Denmark) and in connection with our membership we are subject to an annual audit to verify that we comply with the set of rules established by BFIH, focusing on how we provide our services, perform restore, manage security back-up, etc.

Assessment of the IT security policies

We continuously update our IT security policies, as a minimum once a year.

Organisation of information security

Internal organisation

Delegation of responsibilities for information security

We have a clearly divided organisation in regard to responsibilities; and we have thorough descriptions of responsibilities and roles at all levels, from management to each 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 are able to eliminate or minimise key staff dependency. Tasks are allocated and established via procedures for management of operations.

Contact with specific 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.

Information security in project management

If we find that a project fails to comply with our information security procedures, the project will be adapted in a way that it subsequently matches our standard within information security. If we find that the project is not feasible or amendable without being in conflict with our security policies, then the project will be abandoned.

Mobile devices and teleworking

Mobile devices and communication

We allow our employees to work from home due to, amongst others, operations duties and our policy is that devices (portable, 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 synchronising mails and calendars. We have not implemented security measures other than password protection to secure such devices and user access.

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

Remote work

Access to our network and thereby potentially systems and data is only possible for authorised individuals. Our employees have access via remote workplaces using Remote Desktop and IP restriction.

Human resource security

Prior to employment

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 groups of employees in order to ensure that all employees are aware of their responsibilities. When joining the company, all employees are reviewed and a registrations 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 clearly defines, as part of the contract material, the employee's responsibilities and role.

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 organised on a current 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 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 listed.

Termination or change of employment responsibilities

In the event of termination of employment, we have implemented 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 is revoked. The overall responsibility for all controls related to the termination process lies with the company's CTO.

Asset management

Responsibility for assets

Inventory of assets

Software, servers and network devices, including configuration, are registered for use for documentation, overview of devices, etc. We have a complex network including many systems and customers and to protect against unauthorised access and to ensure a transparent structure, we have prepared documentation describing the internal network with units, names of units, logic composition of networks, etc.

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

Ownership of assets

By means of division of responsibilities central network units, 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 staff 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 is revoked. The overall responsibility for all controls related to the termination process lies with the company's CTO.

Media handling

Management of removable media

We ensure to the widest extent possible that our staff's portable media, e.g. laptops, mobile phones and similar, is 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 control

Business requirements of access control

Access control policy

We have a policy regarding 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.

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 will be 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 to the individual employee and are subject to password policies in order to ensure complexity.

Review of user access rights

For our own users, the company's CTO will periodically, once a year as a minimum, review the company's in-house systems for creation of users and their access level to prevent unauthorised access.

User responsibilities

Use of secret authentication information

According to our IT security policies our employees' passwords are personal and only the user must know the password. Every year the employees sign a document stating that they have read and understood the latest version of our IT security policy. 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 application 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 so that there are restrictions in relation to the design of the password. Passwords must be changed regularly and they must be complex.

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

Physical and environmental security

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

Security of equipment and assets off-premises
We conduct back-up procedures during the night to protect our customers' data and systems if 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 prevent theft, fire, water and temperature deviations.

We annually receive an auditor's opinion covering the physical security at our subcontractor.

The most recent auditor's opinions cover the periods 1/1 2015 through 31/12 2015, and 15/6 2015 through 14/6 2016. The opinions are issued without qualifications.

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 unauthorised staff cannot access confidential data.

Operations security

Operational procedures and responsibilities

Documented operational procedures
Although our organisation 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 in order 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 in order to ensure that changes are made as agreed with customers and are properly planned according to the in-house conditions. Changes are only made on the basis of a qualification of the project, the complexity and assessment of effects on other systems. Moreover, a process is followed regarding development and testing.

Regardless of the change in question, we always ensure as a minimum that:

- All changes are discussed, prioritised 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 company and the 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.

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 will have access hereto.

Capacity management

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

Protection from malware

Controls against malware

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 to be infected with on the Internet via mails etc. We have antivirus systems, systems for monitoring Internet usage, traffic and resources on SaaS platforms, security by means of other technical and central installations (firewall etc.) in place.

Backup

Information backup

We ensure that we can restore systems and data appropriately and correctly 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 like the ones we perform 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 carried forward to our backup systems. Thereby the data is physically separated from our operational systems, and after completion an automatic verification is performed to see 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 Operations follows this. We do not perform pro-active 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, prioritised, 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 are performed simultaneously with the normal log.

Clock synchronisation

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

Installation of software on operational systems

We ensure that only approved and tested updates are installed. In accordance with our membership of BFIH 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 Operations.

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

Management of technical vulnerabilities

Security announcements from DK-CERT are monitored and analysed and if they are found relevant, they are installed on our internal systems within 1 month from release. Additionally, we continuously 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 unauthorised access is of the highest priority to us.

Security of network services

Our customers have access to our systems either via the public networks, where access is allowed via encrypted VPN access, IP-whitelisting or MPLS/VPLS. 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/VPLS). Our customers are responsible for being able to access to the Internet.

Segregation in networks

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

Information transfer policies and procedures

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 passwords to customer systems are sent via mail, but they must be changed at first logon. Forgotten passwords, personal details, 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 or non-disclosure 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 subcontractors and business partners.

System acquisition, development and maintenance

Security requirements of information systems

Information security requirements analysis and specification

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

Change management procedures

We have defined a process for change management in order to ensure that changes are made as agreed with customers and are properly planned according to the in-house conditions. Changes are only made on the basis of 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.

Regardless of the change in question, we always ensure as a minimum that:

- All changes are discussed, prioritised 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 according to the new change in case it is found necessary.

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 has access hereto.

Restriction on changes to software packages

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

Supplier relationships

Management of third party services

Managing changes to supplier services

When changes occur internally in the organisation, including policies and procedures, and amendments 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 visit such third parties regularly, whereby we ensure that the agreed terms are continually fulfilled.

Information security incident management

Management of information security breaches and improvements

Responsibilities and procedures

Our employees are under obligation to keep themselves updated by means of providers' support sites, discussion forums etc. for 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 ASP is responsible for preparing and maintaining procedures that ensure timely and correct intervention in connection with security breaches.

Reporting information security incidents

Our hotline system that we use to handle all issues for customers and internal matters is the same system that we use to handle security incidents. Here we can escalate issues so that some incidents have higher priority than others. Moreover, security incidents identified from own observations, alarms from log and monitoring systems, telephone calls from customers, subcontractors or partners, respectively, are escalated from our hotline to Operations, 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 information 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 in order that action can be taken to address the issue as soon as possible and necessary measures can be taken in accordance with the procedures established.

Business continuity management

Information security aspects of 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.

Via our membership of BFIH (Brancheforeningen for IT-hostingvirksomheder i Danmark – Trade association for IT hosting companies in Denmark) we are under an obligation to be able to re-establish any unit in our data centre within three days. We ensure that this is done by considering the risks, classifying the units in our operations, and having procedures in place that ensure that in relation to our business continuity planning we can replace our operations platform in order to ensure that the services supplied will be re-established in a timely manner.

Testing, maintenance and reassessment of business continuity plans

The plan is tested once or twice annually as part of our business continuity procedure in order for us to ensure that the customers will only experience limited interruption of services in connection with any emergencies.

Compliance

Review of information security

Independent review of information security

A review is performed by an external IT auditor and 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 and sign that they understand and comply with it. We have on-going controls, conducted by our management team, to ensure that our employees comply with the security measures that are specified in our IT security policies, in relation to 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 during the period

Throughout the period of 1/12 2015 to 30/11 2016 few significant changes have occurred. We have increased the competency of our technical staff in terms of new appointments, and moreover, 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. Moreover, any.cloud's customers are, unless otherwise agreed, responsible for:

- Ensuring that the agreed backup level covers the customer's needs
- Periodically reviewing the customer's own users
- 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 A/S, their customers and their auditors.

Scope

We have been engaged to report on any.cloud A/S' description, presented in Section 2. The description, as confirmed by the management of any.cloud A/S in Section 1, covers any.cloud A/S' operating and hosting services in the period 01-12-2015 to 30-11-2016, as well as the design and operation of the controls related to the control objectives stated in the description.

any.cloud A/S' description (Section 2) contains a number of conditions, which the company must comply with according to the company's membership of BFIH (Brancheforeningen for IT-Hostingvirksomheder I Danmark). Our audit has included these conditions and consists, other than of the physical matters, including server hardware, LAN, WAN, and firewalls, of:

- Whether any.cloud A/S implements critical security updates within 2 months of release
- Whether any.cloud A/S can restore units in data centres within 3 days
- Whether any.cloud A/S complies with BFIH's requirements for a "modicum of good hosting".

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, for stating control objectives 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 behaviour.

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 Organisation", 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 organisation involves performing procedures to obtain evidence about the disclosures in the service organisation'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 organisation, 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 organisation

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 organisation 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 organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of 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 controls, as they were designed and implemented throughout the period 01-12-2015 to 30-11-2016, is fair in all material respects
(b) the controls related to the control objectives stated in the description were suitably designed throughout the period 01-12-2015 to 30-11-2016
(c) the controls for the special requirements, caused by the company's membership of BFIH cf. the description in Section 2, were suitably designed throughout the period 01-12-2015 to 30-11-2016
(d) 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 01-12-2015 to 30-11-2016.

Description of tests of controls

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

Intended users and purpose

This assurance report 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. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial statements.

Copenhagen, 19 December 2016

REVI-IT A/S
State authorised public accounting firm

Henrik Paaske
State Authorised Public Accountant

Martin Brogaard Nielsen
IT Auditor, CISA, CRISC, CEO

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 throughout the period 01-12-2015 to 30-11-2016.

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

No.	any.cloud A/S' control	REVI-IT's test	Test results
4.1	Risk assessment is performed periodically and when we introduce changes or implement new systems which we deem relevant in relation to reassessing our general risk assessment. The company's CTO is responsible for the risk assessments and they must subsequently be embedded in and approved by management. It is continuously assessed whether we can reduce risks and take measures to improve our score.	We have enquired about the preparation of a risk analysis, and we have inspected the prepared risk analysis. We have enquired about review of the IT 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.

No.	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. In order to do that, we have introduced policies and procedures ensuring that our deliveries are uniform and transparent. We continuously improve our policies, procedures and operations. We continuously update our IT security policy, as a minimum once a year.	We have enquired about the preparation of an information security policy, and we have inspected the policy. We have enquired about periodic review of the information security policy, and we have checked that the policy has been reviewed during the audit period. Additionally, we have inspected control for periodic review of the document. We have enquired about management approval of the information security policy, and we have inspected documentation for management approval.	No significant deviations noted.

Organisation of information security

Internal organisation

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

No.	any.cloud A/S' control	REVI-IT's test	Test results
6.1	We have a clearly divided organisation in regard to responsibilities; and we have thorough descriptions of responsibilities and roles at all levels, from management to each operations employee. Through continuous documentation and processes we ensure that we are able to eliminate or minimise key staff dependency. Tasks are allocated and established via procedures for management of operations. 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.	We have enquired about allocation of responsibility for information security, and we have inspected documentation for the allocation and maintenance of descriptions of responsibilities. We have enquired about access segregation in relation to function, and we have inspected documentation for differentiated access. We have enquired about guidelines for contact with authorities. We have enquired about contact with interest groups, and we have inspected documentation for contact with DK-CERT. We have enquired about the consideration of information security in project management. We have in spot checks inspected project processes 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
6.2	We allow our employees to work from home due to, amongst others, operations duties and our policy is that devices (portable, etc.) may only be used for work-related purposes and must not be left unattended, etc. Portable devices are protected with logon and encryption. Our employees have access via remote workplaces using Remote Desktop and IP restriction.	We have enquired about mobile device management, and we have inspected the solution. We have enquired 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
7.1	We have procedures in place governing recruitment of employees, ensuring that we recruit the right candidates based on background and skills. When joining the company, all employees are reviewed and a registrations form is followed. In connection with employment all new hires sign a contract. The contract details that the employee must comply with the at all times applicable policies and procedures.	We have enquired about a procedure for hiring new employees, and we have inspected the procedure. We have in spot checks inspected documentation showing that the procedure has been followed. We have enquired about the formalisation 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
7.2	We have a clearly divided organisation in regard to responsibilities; and we have thorough descriptions of responsibilities and roles at all levels, from management to each operations employee. 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 organised on a current 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. 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 listed.	We have enquired about a description of management's responsibility for communicating information security criteria, and we have inspected the description. We have enquired about staff training, and we have in spot checks inspected documentation for participation in courses. We have enquired 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 organisation's interests as part of the process of changing or terminating employment.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
7.3	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.	We have enquired 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 organisational assets and define appropriate protection responsibilities.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
8.1	Software, servers and network devices, including configuration, are registered for use for documentation, overview of devices, etc. The documents, network topologies and similar are continuously updated in the event of changes and are reviewed at least once a year by our network specialists. By means of division of responsibilities and role descriptions central network units, 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. 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 is revoked.	We have enquired about inventories of assets, and we have in spot checks inspected inventories of assets. We have enquired about controls for ensuring assets are updated, and we have inspected the controls in place. We have enquired about an inventory of asset ownership, and we have inspected the inventory. We have enquired about guidelines for the use of assets, and we have inspected the guidelines. We have enquired about a procedure for ensuring the return of handed-out assets, and we have in spot checks inspected the procedure. Additionally, we have in spot checks inspected documentation for the return of assets.	No significant deviations noted.

Media handling **Control objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
8.3	We ensure to the widest extent possible that our staff's portable media, e.g. laptops, mobile phones and similar, have a security configuration 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.	We have enquired about mobile device management, and we have inspected documentation for the solution. We have enquired about a process for disposal of media, and we have inspected the process. We have enquired about transport of physical media.	No significant deviations noted.

Access control

Business requirements of access control **Control objective: To limit access to information and information processing facilities.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
9.1	We have a policy regarding allocation of access. This policy is an integral part of our IT security policy.	We have enquired about a policy for management of access to systems and buildings, and we have inspected the policy. We have enquired 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 unauthorised access to systems and services.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
9.2	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 will be disabled. Allocation of privileges is controlled in connection with our normal user management process. All personal logons are only known to the individual employee and are subject to password policies for securing complexity. For our own users, the company's CTO will periodically, once a year as a minimum, review the company's in-house systems for creation of users and their access level to prevent unauthorised access.	We have enquired about a procedure for creating and disabling users, and we have inspected the procedures. We have in spot checks inspected documentation for creation and disabling of users during the period. We have enquired about a procedure for allocating rights, and we have inspected the procedure. We have enquired about storage of confidential passwords, and we have inspected documentation for adequate storage. We have enquired about a process for periodic review of users, and we have inspected documentation for the latest review.	No significant deviations noted.

User responsibilities **Control objective: To make users accountable for safeguarding their authentication information.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
9.3	Our IT security policy states that our employees' passwords are personal, and only the user is to know the password. Every year the employees sign a document stating that they have read and understood the latest version of our IT security policy.	We have enquired about guidelines for the use of confidential passwords, and we have inspected the guidelines. We have enquired about annual training of staff in relation to information security, and we have inspected documentation for staff training.	No significant deviations noted.

System and application access control **Control objective: To prevent unauthorised access to systems and applications.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
9.4	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. 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 so that there are restrictions in relation to the design of the password. Passwords must be changed regularly and they must be complex.	We have enquired about restrictions on access to data, and we have inspected documentation for restriction. We have enquired about a procedure for secure logon, and we have inspected the solution. We have enquired about a system for password management. We have inspected the solution and selected configurations.	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.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
10.1	Our customers have access to our systems via the public networks, where access is allowed via encrypted VPN access, IP-whitelisting or MPLS/VPLS. Portable devices are protected with logon and encryption.	We have enquired about a policy for the use of encryption, and we have in spot checks inspected documentation for the use of cryptography. We have enquired about administration of encryption keys, and we have inspected documentation for this management.	No significant deviations noted.

Physical and environmental security

Secure areas

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

No.	any.cloud A/S' control	REVI-IT's test	Test results
11.1	We have entered into an agreement with the concerned supplier on housing of our proprietary servers and similar measures are implemented to prevent theft, fire, water and temperature deviations. We annually receive an auditor's opinion covering the physical security at our subcontractor.	We have enquired about an auditor's opinion from the subcontractor for the physical environment, and we have inspected the auditor's opinion for adequate physical security. We have observed that the auditor's opinion from subcontractor respectively covers the period 1 January 2015 to 31 December 2015 and 16 June 2015 to 15 June 2016. We have enquired about periodic review of external location, and we have in spot checks inspected documentation for inspection. We have enquired about the allocation and revocation of access to operations facilities at the subcontractor, and we have in spot checks inspected documentation for the allocation of access to operations facilities. We have inspected the physical environment at any.cloud's offices in order to check the physical security. We have enquired about the delivery of parcels and goods.	No significant deviations noted.

Equipment **Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
11.2	We have entered into an agreement with the concerned supplier on housing of our proprietary servers and similar measures are implemented to prevent theft, fire, water and temperature deviations. The data centre's cooling and fire prevention systems are checked regularly and the back-up power system (UPS) is checked every six months. Systems are installed in the data centre monitoring temperatures and voltages in the server room. We annually receive an auditor's opinion covering the physical security at our subcontractor. All data-carrying devices are destroyed before disposal to 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. Thereby we ensure that unauthorised staff cannot access confidential data.	We have enquired about an auditor's opinion from subcontractor regarding physical environment. We have inspected the auditor's opinion in order to identify observations in relation to physical security; and in relation to this we have, amongst others, checked that there are supporting supplies, and that these are maintained. We have observed that the auditor's opinion from subcontractor respectively covers the period 1 January 2015 to 31 December 2015 and 16 June 2015 to 15 June 2016. We have enquired about periodic review of external location, and we have in spot checks inspected documentation for inspection. Additionally, by means of re-performing the control we have inspected the external location. We have enquired about the securing of cabling, and we have inspected auditor's opinion from supplier. We have enquired about a policy for the disposal of equipment. We have enquired about the securing of unattended user equipment, and we have in spot checks inspected that user equipment is locked at inactivity.	No significant deviations noted.

Operations security

Operational procedures and responsibilities

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

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.1	We ensure via documentation and descriptions that existing or new employees can commence working on a system for which the said person does not have operational or previous experience. The system documentation is updated continuously. Changes are only made on the basis of a qualification of the project, the complexity and assessment of effects on other systems. Moreover, a process is followed regarding development and testing. Via our general monitoring system, we have set limits for when our overall systems, and thereby our customers' systems, must be upscaled with regard to electronic space, response time, etc. 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.	We have enquired about procedures in connection with operations, and we have in spot checks inspected the procedures. We have enquired about controls for updating operations procedures, and we have inspected the control. We have enquired about a procedure for change management, and we have inspected the procedure. We have in spot checks inspected documentation for change management during the period. We have enquired about capacity monitoring, and we have in spot checks inspected documentation for capacity monitoring. We have enquired 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.2	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 to be infected with on the Internet via mails etc. We have antivirus systems, systems for monitoring Internet usage, traffic and resources on SaaS platforms, security by means of other technical and central installations (firewall etc.) in place.	We have enquired about measures to protect against malware. We have enquired 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.3	We ensure that we can restore systems and data appropriately and correctly 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 have defined guidelines as to how we perform backups.	We have enquired about the configuration of backup, and we have in spot checks inspected documentation for the setup. We have enquired about the storage of backup, and we have inspected the auditor's opinion from subcontractor in order to verify that backup is stored securely. Additionally, we have inspected documentation for backup being stored in a separate location in relation to the production environment. We have enquired 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.4	We have set up monitoring and logging of network traffic and Operations follows this. We follow up if we suspect that an incident can be related to issues addressed in the log. Logs are uploaded to our log server. Administrator logs are performed simultaneously with the normal log. We use NTP servers from the Internet, which all servers are synchronised up against.	We have enquired about the logging of user activity. We have in spot checks inspected the logging configurations. We have enquired about the securing of log information, and we have inspected the solution. We have enquired about synchronisation 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.5	By means of our patch process we ensure that only approved and tested updates are installed. In the event of major changes, this will be discussed at internal meetings in Operations. Moreover, our staff is aware of the policy regarding software downloads.	We have enquired about guidelines for installation of software on operations systems, and we have inspected the guidelines. We have enquired about timely updates to operations systems, and we have inspected documentation for updates of operations systems, which is in accordance with BFIH's requirements.	No significant deviations noted.

Technical vulnerability management **Control objective: To prevent exploitation of technical vulnerabilities.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
12.6	Security announcements from DK-CERT are monitored and analysed and if they are found relevant, they are installed on our internal systems within 1 month from release. Additionally, we continuously perform a risk assessment of our in-house solutions.	We have enquired about management of technical vulnerabilities, and we have inspected documentation for this management. We have enquired 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.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
13.1	Our customers have access to our systems either via the public networks, where access is allowed via encrypted VPN access, IP-whitelisting or MPLS/VPLS. 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. Our network is divided into various segments whereby we ensure that our internal network is segregated from the customers' networks.	We have enquired about measures to secure network and network services. We have inspected documentation for the establishment of firewall and patching of firewall. We have enquired 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 organisation and with any external entity.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
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. 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 subcontractors and business partners.	We have enquired about a policy for information transfer, and we have inspected the policy. We have enquired about guidelines for handling electronic messages, and we have inspected the guidelines. We have enquired about the establishment of confidentiality agreements, and we have in spot checks inspected documentation for entered confidentiality agreements.	No significant deviations noted.

Supplier relationships

Information security in supplier relationships

Control objective: To ensure protection of the organisation's assets that are accessible by suppliers.

No.	any.cloud A/S' control	REVI-IT's test	Test results
15.1	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 visit such third parties regularly, whereby we ensure that the agreed terms are continually fulfilled.	We have enquired about the formalisation of supplier agreements, and we have inspected the agreement in order to check the consideration of information security. We have inspected an auditor's opinion from subcontractor in order to identify adequate security.	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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
15.2	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 visit such third parties regularly, whereby we ensure that the agreed terms are continually fulfilled.	We have enquired about monitoring of subcontractors, and we have inspected documentation for monitoring. We have enquired about change management at subcontractors.	No significant 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.

No.	any.cloud A/S' control	REVI-IT's test	Test results
16.1	There are formally appointed ASPs and the requirements they are subject to are clearly and formally defined. The ASP is responsible for preparing and maintaining procedures that ensure timely and correct intervention in connection with security breaches. Our employees and external partners are, via the entered contracts and agreements, under an obligation to report any security incident to their immediate superior in order that action can be taken to address the issue as soon as possible and necessary measures can be taken in accordance with the procedures established.	We have enquired 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 enquired about guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines. We have enquired about a procedure for assessing, reacting to and evaluating information security breaches, and we have inspected the procedure. We have enquired about information security incidents during the period, and we have in spot checks inspected documentation for the handling of information security breaches.	No significant deviations noted.

Information security aspects of business continuity management

Information security continuity

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

No.	any.cloud A/S' control	REVI-IT's test	Test results
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. The plan and the procedures are embedded in our operations documentation and procedures. The plan is tested once or twice annually as part of our business continuity in order for us to ensure that the customers will only experience limited interruption of services in connection with any emergencies.	We have enquired 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 inspected documentation for management approval and periodic control of review of the business continuity plan. We have enquired about test of the business continuity plan, and we have inspected documentation for test of the business continuity plan.	No significant deviations noted.

Redundancies **Control objective: To ensure availability of information processing facilities.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
17.2	any.cloud is hosted in InterXion Danmark in Ballerup and Global Connect in Taastrup.	We have enquired about the availability of operations systems, and we have inspected the established measures. We have enquired about redundancy on Internet connections, and we have inspected documentation for redundancy on Internet connections cf. BFIH's requirements.	No significant deviations noted.

Compliance

Information security reviews **Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.**			
No.	any.cloud A/S' control	REVI-IT's test	Test results
18.2	Our employees read the IT security policies once a year as a minimum and sign that they understand and comply with it. We have on-going controls, conducted by our management, to ensure that our employees comply with the security measures that are specified in our IT security policy, in relation to the physical as well as the logical conditions. Furthermore, we have controls ensuring compliance with monitoring and security.	We have enquired about independent evaluation of the information security. We have enquired about internal controls for ensuring compliance with security policy and procedures, and we have inspected selected controls. We have enquired about periodic control of technical compliance, and we have inspected documentation for monitoring.	No significant deviations noted.