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 01-12-2014 to 30-11-2015

ISAE 3402-II

any.cloud A/S

CVR no.: 31 16 15 09

December 2015

This report was originally prepared in Danish.

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

REVI-IT A/S • state authorised public accounting firm
Lyngbyvej 20 • DK-2100 Copenhagen • Phone 3311 8100 • Fax 3311 8103 • info@revi-it.dk • revi-it.dk • CVR-no. 3098 8531

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 01-12-2014 to 30-11-2015. 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 for processing and reporting customer transactions.

(ii) Provides relevant details of changes in the service organisation's system throughout the period 01-12-2014 to 30-11-2015

(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 01-12-2014 to 30-11-2015. 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 01-12-2014 to 30-11-2015.

Copenhagen, December 18, 2015

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 relations are not included in this description.

any.cloud

any.cloud was founded in 2007 and is a sister company of the consultancy firm any.mac A/S. any.cloud supplies professional ISO certified cloud services to the Danish business community. This is any.cloud's third ISAE3402 Type II report.

any.cloud has primary hosting at InterXion Danmark in Ballerup's 3,500 square metre-facilities, being a European provider of cloud and operator independent data centres with more than 39 data centres in 11 countries. any.cloud offers co-location via a closed network in the 27 data centre-wide, IBM-owned company Softlayer, providing solutions through this business world-wide.

We offer all relevant security measures, e.g. Inergen, cooling, redundant power sources and fibre lines and fully equipped monitoring systems.

any.cloud is subject to stringent control measures, high security requirements and transparency requirements in relation to the quality and security of IT hosting services.

any.cloud is headquartered in Denmark and we have offices in Poland and the Czech Republic.

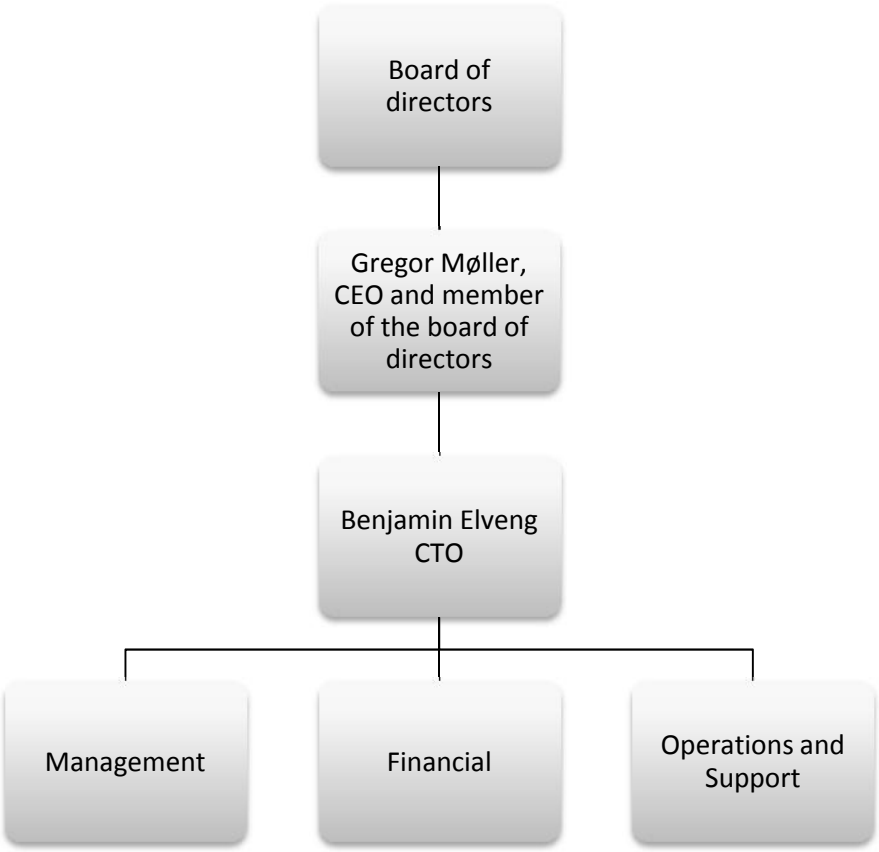
any.cloud – IT made simple

any.cloud offers the following basic products:

- VPS (Virtual Private Server)
- Virtual hybrid solution with optional DRaaS (Disaster Recovery as a Service)
- Security products
- MPLS and fibre infrastructure.

Organisation and responsibilities

any.cloud has a simple and transparent corporate structure.



any.cloud employs 13 persons, covering the departments Management, Financial and Operations and Support. Moreover, 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 are only working on the hosting infrastructure.

Support receives all inquiries and solves customer issues or forwards it to Operations for processing.

Operations thus functions both as 2nd line support for hotline and 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 ongoing risk assessment of our business and especially our cloud services. This allows 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 find are relevant, we re-assess 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 had to introduce 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 any employee and any delivery.

Our methods for implementation of controls are defined according to ISO 27002 (framework for management of information security) and they are 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) 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 at least once a year.

Organisation of information security

Internal organisation

Delegation of responsibilities for information security
We have a clearly divided organisation as regards responsibilities; and we have thorough descriptions of responsibilities and roles at all levels from top to bottom in our organisation.

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 exclude or minimise key staff dependency. Tasks are allocated and established via procedures for control and management of operations.

Contact with specific interest groups
We have established contact to a hotline at DK-CERT with whom we have entered into 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 either 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 we have put a policy in place that devices (portable, etc.) may only be used for work-related purposes and must not be left unattended, etc. Portable devices are logon and encryption protected.

We have given access to the possibilities that we and our customers can use mobile devices (smartphones, tablets, etc.) to synchronise 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 drafted 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 personal and customer relations, 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 include 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, though once a year as a minimum, to ensure that relevant employees and possibly 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 hereof.

Disciplinary process

General terms of employment, including confidentiality regarding personal and customer relations, 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.

Responsibilities in the event of termination

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 by 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 updated in the event that changes are introduced and are reviewed at least once a year by our network specialists.

Ownership of assets

Central network units, servers, peripherals, systems and data are dedicated to ASPs in our organisation via allocation of responsibilities and description of roles. 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 put a thorough 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, are 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 security measures.

Access control

Business requirements of access control

Access control policy

We have a policy in place 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 therefore responsible for the creation and termination of user accounts.

All users must be attributable to an individual, 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 subject to password policies to secure the 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. Since 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 different access privileges and they will therefore only have access to the systems and data that are relevant for their work performance.

Password management system
All employees across both client systems and proprietary systems have restrictions as regards passwords. All users have a password and system-wise 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 UPS is checked every six months. The systems installed in the data centre monitor 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 are unavailable.

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

We receive the auditor's opinion every year covering the physical security at our subcontractor.

The most recent auditor's opinion we have received covers the period of 01/01-2014 to 31/12-2014. The opinion is given without qualification.

Secure disposal or re-use of equipment
All data-carrying devices are destroyed before disposal to ensure that no data is available.

Unattended user equipment
All internal user accounts are centrally managed to go in screen lock mode after max. 2 minutes of inactivity. This helps us secure that unauthorised staff will not have access to 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 documentations 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 his/her 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 business 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 as regards electronic space, response time, etc. When we set up new systems, functionality testing needs to be carried out, including capacity and performance testing. A regular procedure is prepared for reporting of 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 tested how systems and data in practice can be restored. We keep a log of these tests in order that we can follow up on whether we can change our procedures and processes to improve our solution.

Unless otherwise agreed with our customers, we perform a 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 after that enter it into the log.

Logging and monitoring

Event logging

We have set up monitoring and logging of traffic on the network and Operations 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, 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 at the same time as 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 via our patch process. In accordance with our membership of BFIH we ensure that critical patches that have an effect on security will never be installed later than 2 months after they are released. In the event of major changes, this will be discussed at in-house meetings in Operations.

Moreover, our staff is aware of the policies 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 after release. Moreover, 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 high 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-white listing or MPLS/VPLS. Access and communication between our servers and our co-location only takes place in a closed network.

Only approved network traffic (inbound) is allowed by 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' network. Moreover, the services with sensitive data are placed in special, secured environments.

Information transfer policies and procedures

External data communication is only performed via mails as our customers' access and use of our servers are not considered external data communication.

Initial passwords to customer systems are sent via mail, but it 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 an 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, a number of analyses and research will be carried out in order to ensure it complies with best practice for hardening.

System change control 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 the 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. Via access controls we ensure that only authorised personnel will have 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 as it is possible.

Supplier relationships

Management of third-party services

Managing changes to supplier services

When internal changes occur 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 carried out 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 can ensure that the agreed terms are still fulfilled.

Information security incident management

Management of information security breaches and improvements

Responsibilities and procedures

Our employees are under an obligation to keep themselves updated by using the support websites from the producers, discussion forums, etc. to locate the weaknesses of the systems we are using and supplying.

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 events

Our hotline system that we use to handle all issues for customers and internal relations 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 caused from own observations, alarms from log and monitoring systems, telephone calls from customers, sub-suppliers 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 contracts and agreements we have entered into, 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.

Information security incident 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 emergency plan is embedded in the IT risk analysis and is updated at least once a year further to conducting 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) we are under an obligation 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 emergency planning we can replace our operations platform in order that the services supplied will be timely re-established.

Testing, maintenance and reassessment of business continuity plans

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

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 ongoing controls, conducted by our management team, to ensure that our employees comply with the security measures that are specified in our IT security policies, both as regards the physical and 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 an external system monitoring availability of all our services with another ISO certified hosting provider. Furthermore, we have controls ensuring compliance with monitoring and security.

Changes during the period

During the period of 01/12-2014 to 30/11-2015 only few changes have occurred. We have increased the competency of our technical staff in terms of new staff and, moreover, we have:

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

Supplementary controls

any.cloud's customers are, unless otherwise agreed, responsible for establishing a connection to any.cloud'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's at any time current Service Level Agreement, which can be found on any.cloud'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 management, covers any.cloud A/S' operating and hosting services in the period 01-12-2014 to 30-11-2015, 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-Hostingvirksomeder 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 centre within 3 days.

This assurance report is prepared according to the inclusive method and thus comprises the management's description of control objectives and related control activities at any.cloud A/S for all areas of the general IT controls, which can be attributed to the delivered services.

any.cloud A/S' responsibility

any.cloud A/S is responsible for preparing the description (section 2) and the related assertion (section 1) including the completeness, accuracy and method of presentation of the description and assertion. 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.

Our independence and quality control

We have complied with the requirements to independence and other ethical rules in IESBA's Code of Ethics, which is based on fundamental principles of integrity, objectivity, professional competences and appropriate care, confidentiality, and professional conduct.

The company employs ISQC 1 and maintains therefore a comprehensive system for quality control, including documented policies and procedures for the compliance with ethical rules, professional standards, as well as existing requirements according to legislation and other regulations.

REVI-IT A/S' responsibility

Based on our procedures, our responsibility is to express an opinion on any.cloud'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 the controls, as they were designed and implemented in the entire period of 01-12-2014 to 30-11-2015 is fair in all material respects
(b) the controls related to the control objectives stated in the description were suitably designed in the entire period of 01-12-2014 to 30-11-2015 in all material respects
(c) the controls for the special requirements, as prompted by the company's membership of BFIH cf. the description in section 2, were suitably designed in the entire period of 01-12-2014 to 30-11-2015
(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 entire period of 01-12-2014 to 30-11-2015.

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' 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, December 18, 2015

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 performed, tests and results thereof

The following overview is provided to facilitate an understanding of the effectiveness of the controls implemented by any.cloud A/S. Our test 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 01-12-2014 to 30-11-2015.

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

Moreover, our assurance report 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.

According to our knowledge of any.cloud A/S' organisation and standard hosting services, we have assessed that control area 14, System acquisition, development and maintenance, from ISO 27002:2013, is not relevant for review in relation to the company's standard hosting services, as the mentioned area concerns matters in relation to system development.

Risk assessment and management

Risk assessment

No.	Control objective	REVI-IT's test	Test results
4.1	To ensure that the company periodically performs an analysis and assessment of the IT risk profile.	We have enquired about the preparation of a risk assessment, and we have inspected the prepared risk assessment. We have enquired about evaluation of the IT risk analysis during the period, and we have verified that it has been reviewed and approved by management during the audit period.	No significant deviations have been noted.

Information security policies

Management direction for information security

No.	Control objective	REVI-IT's test	Test results
5.1	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.	We have enquired about the preparation of an information security policy, and we have inspected the document. We have enquired about periodic review of the information security policy, and we have inspected that the document has been reviewed during the audit period. Furthermore, we have inspected the control for periodic review of the document. We have enquired about management approval of the information security policy and have inspected the documentation for management approval.	No significant deviations have been noted.

Organisation of information security

Internal organisation

No.	Control objective	REVI-IT's test	Test results
6.1	To establish a management framework to initiate and control the implementation and operation of information security within the organisation.	We have enquired about the assignment of responsibilities for the information security and have inspected documentation for the assignment and maintenance of responsibility descriptions. We have enquired about segregation of access 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 have inspected documentation for contact with DK-CERT. We have enquired about consideration of information security in project management. We have inspected project processes in spot checks and verified that information security is considered.	No significant deviations have been noted.

Mobile devices and teleworking

6.2	To ensure the security of teleworking and use of mobile devices.	We have enquired about the management of mobile devices, and we have inspected the solution. We have enquired about the security of teleworking, and we have inspected the solution.	No significant deviations have been noted.

Human resource security

Prior to employment

No.	Control objective	REVI-IT's test	Test results
7.1	To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	We have enquired about a procedure for hiring new employees, and we have inspected the procedure. Furthermore, we have in spot checks inspected documentation for the process being 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 have been noted.

During employment			
7.2	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.	We have enquired about a description of management's responsibility for disseminating information security criteria, and we have inspected the description. We have enquired about staff training, and we have in spot checks inspected documentation for course participation. We have enquired about guidelines for a disciplinary process, and we have inspected the guidelines.	No significant deviations have been noted.
Termination and change of employment			
7.3	To protect the organisation's interests as part of the process of changing or terminating employment.	We have enquired about the formalisation of obligations after termination of employment, and we have in spot checks inspected a formalised agreement.	No significant deviations have been noted.

Asset management

Responsibility for assets			
No.	Control objective	REVI-IT's test	Test results
8.1	To identify organisational assets and define appropriate protection responsibilities.	We have enquired about inventories of assets, and we have in spot checks inspected inventories of assets. We have enquired about a directory of ownership of assets, and we have inspected the directory. We have enquired about guidelines for the use of assets, and we have inspected the guidelines. We have enquired about a procedure for the return of previously issued assets, and we have inspected the procedure.	It has not been possible to test the effectiveness of the procedure for the return of assets as no employees have been terminated from the company during the audit period.
Media handling			
8.3	To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.	We have enquired about the management of portable media, and we have inspected documentation for the solution. We have enquired about guidelines for the disposal of media. We have enquired about transport of portable media.	No significant deviations have been noted.

Access control

Business requirements of access control

No.	Control objective	REVI-IT's test	Test results
9.1	To limit access to information and information processing facilities.	We have enquired about a policy for managing access to systems and premises, and we have inspected the policy. We have enquired about the management of access to network and network services, and we have inspected the solution.	No significant deviations have been noted.

User access management

9.2	To ensure authorised user access and to prevent unauthorised access to systems and services.	We have enquired about procedures for creating and removal of users, and we have inspected the procedures. We have in spot checks inspected documentation for the creation and removal of users. We have enquired about a process for the allocation of rights, and we have inspected the process. We have enquired about monitoring of the use of privileged access rights, and we have in spot checks inspected documentation for monitoring. We have enquired about the storage of secret authentication information, and we have inspected documentation for adequate storage. We have enquired about a process for periodical review of users, and we have inspected documentation for the latest review. We have enquired about a procedure for the removal of access rights, and we have inspected the procedure.	It has not been possible to test the effectiveness of the removal of access rights as no employees have been terminated from the company during the audit period. However, we have observed that a procedure exists.

User responsibilities

9.3	To make users accountable for safeguarding their authentication information.	We have enquired about guidelines for the use of secret authentication information, and we have inspected the guidelines.	No significant deviations have been noted.

System and application access control			
9.4	To prevent unauthorised access to systems and applications.	We have enquired about restricting access to data, and we have inspected documentation for the restriction. We have enquired about a procedure for secure log-on, and we have inspected the solution. We have enquired about a password management system. We have inspected the solution and selected configurations.	No significant deviations have been noted.

Cryptography

Cryptographic controls			
No.	Control objective	REVI-IT's test	Test results
10.1	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.	We have enquired about a policy for the use of encryption, and we have in spot checks inspected the use of cryptography.	No significant deviations have been noted.

Physical and environmental security

Secure areas

No.	Control objective	REVI-IT's test	Test results
11.1	To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.	We have enquired about an assurance report from subcontractor of physical matters, and we have inspected the assurance report for adequate physical security. We have observed that the assurance report from subcontractor covers the period January 1, 2014 to December 31, 2014. We have enquired about periodical inspection of external location, and we have in spot checks inspected documentation for inspection. Furthermore, we have, by re-performance of the control, inspected the external location. We have enquired about the granting and revocation of access to operations facilities at subcontractor, and we have in spot checks inspected documentation for the granting of access to operations facilities. We have inspected the physical conditions 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 have been noted.

Equipment			
11.2	To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.	We have enquired about an assurance report from subcontractor of physical matters. We have inspected the assurance report in order to identify remarks in relation to the physical security, and we have, i.a., checked that there are supporting supplies and that these are maintained. We have observed that the assurance report from subcontractor covers the period January 1, 2014 to December 31, 2014. We have enquired about periodical review of external location, and we have in spot checks inspected documentation for review. Furthermore, we have, by re-performance of the control, inspected the external location. We have enquired about the securing of cables, and we have inspected the assurance report from subcontractor. We have enquired about a policy for the disposal of equipment. We have enquired about the security of unattended user equipment, and we have in spot checks inspected that user equipment is locked when inactive.	No significant deviations have been noted.

Operations security

Operational procedures and responsibilities

No.	Control objective	REVI-IT's test	Test results
12.1	To ensure correct and secure operation of information processing facilities.	We have enquired about procedures in connection with operations and have in spot checks inspected the procedures. We have enquired about change management and 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 have been noted.

Protection from malware			
12.2	To ensure that information and information processing facilities are protected against malware.	We have enquired about precautionary measures against malware. We have enquired about the use of anti-virus programs, and we have inspected documentation for the use.	No significant deviations have been noted.
Backup			
12.3	To protect against loss of data.	We have enquired about the configuration of backup, and we have in spot checks inspected documentation for setup. We have enquired about the storage of backup and have inspected the assurance report from subcontractor in order to ensure that backup is stored securely. We have enquired about test of restoration from backup files, and we have inspected documentation for restore test.	No significant deviations have been noted.
Logging and monitoring			
12.4	To record events and generate evidence.	We have enquired about logging user activity, and we have in spot checks inspected the logging configurations. We have enquired about the securing of log information and have inspected the solution. We have enquired about synchronisation up against an adequate clock server, and we have inspected the solution.	No significant deviations have been noted.
Control of operational software			
12.5	To ensure the integrity of operational systems.	We have enquired about guidelines for the installation of software on operational systems, and we have inspected the guidelines. We have enquired about timely updating of operational systems, and we have inspected documentation for updating operational systems, which is in compliance with BFIH's requirements.	No significant deviations have been noted.
Technical vulnerability management			
12.6	To prevent exploitation of technical vulnerabilities.	We have enquired about the management of technical vulnerabilities, and we have inspected the document for the management. We have enquired about management of access to program installation, and we have inspected documentation for the restriction of users with program installation rights.	No significant deviations have been noted.

Communications security

Network security management

No.	Control objective	REVI-IT's test	Test results
13.1	To ensure the protection of information in networks and its supporting information processing facilities.	We have enquired about precautionary measures for the protection of network and network services. We have inspected documentation for the setting-up of firewall as well as patching of firewall. We have enquired about securing network services and have inspected documentation for adequate security. We have enquired about network segregation and have inspected documentation for segregation.	No significant deviations have been noted.

Information transfer

13.2	To maintain the security of information transferred within an organisation and with any external entity.	We have enquired about policies and procedures for information transfer. We have enquired about guidelines for transferring confidential information. We have enquired about the establishment of confidentiality agreements, and we have inspected documentation for the establishment.	No significant deviations have been noted.

Supplier relationships

Information security in supplier relationships

No.	Control objective	REVI-IT's test	Test results
15.1	To ensure protection of the organisation's assets that are accessible by suppliers.	We have enquired about the formalisation of supplier agreements, and we have inspected the agreement in order to inspect considerations in relation to information security. We have inspected an assurance report from subcontractor for identifying adequate security.	No significant deviations have been noted.

Supplier service delivery management

15.2	To maintain an agreed level of information security and service delivery in line with supplier agreements.	We have enquired about the monitoring of subcontractors, and we have inspected documentation for monitoring. We have enquired about change management at subcontractors.	No significant deviations have been noted.

Information security incident management

Management of information security incidents and improvements

No.	Control objective	REVI-IT's test	Test results
16.1	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.	We have enquired about responsibilities and procedures at information security incidents, and we have inspected documentation for division of responsibilities. Furthermore, 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 these guidelines. We have enquired about information security incidents during the period. We have enquired about a procedure for assessment, reaction and evaluation of information security incidents, and we have inspected the procedure.	The company has a procedure for the management of information security incidents. However, it has not been possible to test the effectiveness of the procedure, as there have not been any information security incidents during the period.

Information security aspects of business continuity management

Information security continuity

No.	Control objective	REVI-IT's test	Test results
17.1	Information security continuity should be embedded in the organisation's business continuity management systems.	We have enquired about the preparation of a contingency plan for ensuring operational continuity in connection with failures and similar, and we have inspected the plan. We have enquired about a test of the contingency plan and implementation of compensating steps in connection with the test of the contingency plan, and we have inspected documentation for test and implementation of compensating steps.	No significant deviations have been noted.

Redundancies

17.2	To ensure availability of information processing facilities.	We have enquired about the availability of operational systems, and we have inspected the established precautionary measures.	No significant deviations have been noted.

Compliance

Information security reviews

No.	Control objective	REVI-IT's test	Test results
18.2	To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.	We have enquired about independent evaluation of the information security, and we have inspected that this is performed. We have enquired about an internal control to ensure compliance with security policy and procedures, and we have inspected selected controls. We have enquired about periodical control of technical compliance.	No significant deviations have been noted.