revi-it

Building a safer society through compliance

Assurance report

any.cloud A/S

ISAE 3402 type 2 assurance report on general it-controls for
the period 1 December 2019 to 30 November 2020 related to their hosting services

REVI-IT A/S | www.revi-it.dk
Højbro Plads 10, DK-1200 Copenhagen K
CVR: 30 98 85 31 | Tel. 33 11 81 00 | info@revi-it.dk
www.dpo-danmark.dk | www.revi-cert.dk

February 2021

Table of contents

Section 1: Description of any.cloud A/S' services in connection with hosting services, and related general it-controls

Description of any.cloud A/S' services in connection with hosting services

The following is a description of any.cloud A/S' hosting services which are included in the general it-controls of this assurance report. The report includes general processes and system setups etcetera, with any.cloud A/S. Processes and system setups etcetera, individually agreed with any.cloud A/S' customers, are not included in this report. Assessment of customer specific processes and system setups etcetera, will be stated in specific assurance reports for customers who may have ordered such.

Controls in the application systems are not included in this report.

Introduction

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

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

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

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

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

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

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

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

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

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

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

Organization and responsibility

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

CEO

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

COO

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

CFO

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

CSO

Responsible for sale of all products, and sales staff.

Risk assessment

IT-risk analysis

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

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

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

Management of security risks

Procedure for risk management

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

Information security policy

IT security policy document

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

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

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

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

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

Assessment of the IT security policy

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

Internal organisation

Delegation of responsibility for information security

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

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

Segregation of duties

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

Contact with special interest groups

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

Information security as part of project management

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

Mobile devices and teleworking

Mobile devices and communication

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

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

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

Remote working

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

Human resource security

Screening

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

Terms and conditions of employment

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

During employment

Management responsibilities

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

Information security awareness, education, and training

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

Disciplinary process

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

Termination or change of employment responsibilities

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

Asset Management

Asset inventory

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

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

Ownership of assets

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

Acceptable use of assets

This is described in the employee manual.

Return of assets

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

Management of removable media

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

Access management

Access control policy

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

User access management

User account creation and termination procedures

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

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

Allocation of rights

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

Management of secret authentication information of users

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

Review of user access rights

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

User responsibilities

Use of secret authentication information

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

System and data access control

Information access restriction

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

Password management system

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

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

Physical and environmental security

Equipment maintenance

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

Securing equipment and assets off-premises

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

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

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

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

Secure disposal or re-use of equipment

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

Unattended user equipment

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

Operations security

Documented operating procedures

Although our 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 to ensure that the key responsible employee is responsible for communicating practical issues to their colleagues. The system documentation is updated continuously.

Change management

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

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

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

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

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

Capacity management

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

Protection against malware and DDoS

Controls against malware and DDoS

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

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

Backup

Information backup

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

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

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

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

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

Logging and monitoring

Event logging

We have set up monitoring and logging of network traffic, and our operations department follows this. We do not perform proactive monitoring of logged incidents, but we follow up if we suspect that an incident can be related to issues addressed in the log. For management of monitoring and follow-up on incidents we have implemented formal incident and problem management procedures to safeguard that incidents are registered, prioritized, managed, escalated and that necessary actions are taken. The process is documented in our hotline system.

Protection of log information

Logs are uploaded to our log server.

Administrator and operator log

Administrator logs occur simultaneously with the normal log.

Time synchronization

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

Managing software on operating systems

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

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

Management of technical vulnerabilities

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

Communications security

Network controls

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

Securing network services

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

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

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

Segregation of networks

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

Policies and procedures for data transfer

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

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

Confidentiality agreements

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

System acquisition, development, and maintenance

Information security requirements analysis and specification

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

Change management procedures

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

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

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

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

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

Restriction on changes to software packages

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

Supplier relationships

Management of changes to services

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

Monitoring of third-party services

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

Information security incident management

Responsibilities and procedures

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

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

Reporting of information security breaches

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

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

Reporting security weaknesses

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

Business continuity management

Information security continuity

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

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

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

Testing, maintenance, and reassessment of business continuity plans

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

Compliance

Independent review of information security

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

Compliance with security policies and standards

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

Technical compliance review

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

Changes in the period

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

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

Complementary controls

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

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

Section 2: any.cloud A/S' statement

The accompanying description has been prepared for customers who have used any.cloud A/S' hosting services, and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Any.cloud A/S is using subservice organisations Microsoft Azure, InterXion and IBM Cloud. This assurance report is prepared in accordance with the carve-out method and any.cloud A/S' description does not include control objectives and controls within Microsoft Azure, InterXion and IBM Cloud.

Any.cloud A/S confirms that:

(a) The accompanying description in Section 1 fairly presents the general it-controls related to any.cloud A/S' hosting services, processing customer transactions for the period 1 December 2019 to 30 November 2020 criteria used in making this statement were that the accompanying description:

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

- The type of services provided
- The procedures within both information technology and manual systems, used to manage the general it-controls
- 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 the 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 relevant to general it-controls

(ii) Contains relevant information about changes in the general it-controls, performed during the period 1 December 2019 to 30 November 2020

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period 1 December 2019 to 30 November 2020. 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 used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, during the period from 1 December 2019 to 30 November 2020

Copenhagen, 25 February 2021
any.cloud A/S

Gregor Møller
CEO

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

To any.cloud A/S, their customers, and their auditors.

Scope

We have been engaged to report on any.cloud A/S' description in Section 1 of its system for delivery of any.cloud A/S' services throughout the period 1 December 2019 to 30 November 2020 (the description) and on the design and operation of controls related to the control objectives stated in the description.

Any.cloud A/S is using subservice organisations Microsoft Azure, InterXion and IBM Cloud. This assurance report is prepared in accordance with the carve-out method and any.cloud A/S' description does not include control objectives and controls within Microsoft Azure, InterXion and IBM Cloud.
Some of the control objectives stated in any.cloud A/S' description in Section 1 of general it-controls, can only be achieved if the complementary controls with the customers (or the specific customer) have been appropriately designed and works effectively with the controls with any.cloud A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Any.cloud A/S' responsibility

any.cloud A/S is responsible for preparing the description (section 1) and accompanying statement (section 2) 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; stating the 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.

REVI-IT A/S applies International Standard on Quality Control 1[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.

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

REVI-IT A/S' responsibility

Our responsibility is to express an opinion on any.cloud A/S' description (Section 1) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board.

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 judgement, 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.

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 1, 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 their 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.

Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

Opinion

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

(a) The description of the controls, as they were designed and implemented throughout the period 1 December 2019 to 30 November 2020, is fair in all material respects.

(b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 December 2019 to 30 November 2020 in all material respects.

(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 1 December 2019 to 30 November 2020.

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) including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used any.cloud A/S 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 reporting.

Copenhagen, 25 February 2021

REVI-IT A/S
State authorised public accounting firm

	Christian Riis
Henrik Paaske	Christian H. Riis
State Authorised Public Accountant	Partner, CISA

Section 4: Control objectives, controls, and service auditor testing

4.1. Purpose and scope

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.

This statement is issued according to the carve-out method and therefore does not include controls of any.cloud A/S' subservice organizations.

Our statement, does not apply to controls, performed at any.cloud A/S' customers.

4.2. Tests

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

Method	General description
Inquiries	Interview with appropriate personnel at any.cloud A/S regarding controls.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Furthermore, it is assessed whether controls are adequately monitored and controlled in appropriate intervals.
Re-performance	Re-performance of controls to verify that the control is working as assumed.

4.3. Results of tests

Below, we have listed the tests performed by REVI-IT as basis for the evaluation of the general it-controls with any.cloud A/S.

A.4 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		We have inquired about the preparation of a risk analysis and we have inspected the risk analysis. We have inquired about evaluation of the IT risk profile within the period and we have inspected documentation that this has been reviewed and approved by management during the period.	No deviations noted.

A.5 Information security policies

A.5.1 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
5.1.1	*Policies for information security.* A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.	We have inspected the information security policy and we have inspected documentation for management approval of the information security policy.	No deviations noted.
5.1.2	*Review of policies for information security.* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inspected the procedure for periodic review of the information security policy. We have inspected that the information security policy has been reviewed to ensure that it still is suitable, adequate, and effective.	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation

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

No.	any.cloud A/S' control	REVI-IT's test	Test results
6.1.1	*Information security roles and responsibilities.* All information security responsibilities are defined and allocated.	We have inspected the organisation chart. We have inquired about the guidelines for information security roles and responsibilities.	No deviations noted.
6.1.2	*Segregation of duties.* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organizations' assets.	We have inspected procedures regarding granting and maintenance of segregation of duties and functions. By inquiries and inspection of system data, we have investigated whether operating staff, only have access to administering rights on systems of which they are responsible.	No deviations noted.
6.1.3	*Contact with authorities* Appropriate contacts with relevant authorities are maintained.	We have inspected the policy for maintenance of regulations concerning contact with relevant authorities.	No deviations noted.
6.1.4	*Contact with special interest groups* Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.	We have inspected the procedure regarding maintenance of rules for appropriate contact with special interest groups, security fora and professional organisations.	No deviations noted.
6.1.5	*Information security in project management.* Information security is addressed in project management, regardless of the type of project.	We have inspected the procedure for project management to ensure that information security is addressed.	No deviations noted.

A.6.2 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**
6.2.1	*Mobile device policy.* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected policy for securing of mobile devices. We have inspected, that technical controls for securing of mobile devices have been defined. We have – by sample check – inspected that technical controls are implemented on mobile devices.	No deviations noted.
6.2.2	*Teleworking.* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected policy to secure teleworking, and we have inspected the underlaying security measures for protection of remote workspaces.	No deviations noted.

A.7 Human ressource security

A.7.1 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
7.1.1	*Screening* Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inquired into the procedure for employment of new employees and the security measures needed in the process. We have inspected a selection of contracts with employees to determine whether the procedure regarding background check has been followed.	No deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organization's responsibilities for information security.	We have inspected a selection of contracts with employees and consultants to determine whether these are signed by the employees.	No deviations noted.

A.7.2 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
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	We have inquired about procedure concerning establishing requirements for employees and partners. We have inquired that management has required that employees observe the IT-security policy.	No deviations noted.
7.2.2	*Information security awareness education and training* All employees of the organization and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organizational policies and procedures as relevant for their job function.	We have inquired about procedures to secure adequate training and education (awareness training). We have inspected documentation for activities developing and maintaining security awareness with employees.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to take action against employees who have committed an information security breach.	We have inspected sanctioning guidelines and we have inspected that the guidelines have been communicated.	No deviations noted.

A.7.3 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
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment. We have inspected documentation, that information security has been defined and communicated.	No deviations noted.

A.8 Asset management

A.8.1 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
8.1.1	*Inventory of assets* Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	We have inspected asset listings.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected record of asset ownership.	No deviations noted.
8.1.3	*Acceptable use of assets.* Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.	We have inquired about asset use guidelines and we have inspected the guidelines.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inquired into the procedure for securing the return of assets delivered, and we have inspected the procedure.	No deviations noted.

A.8.2 Classification of information
Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation.

No.	any.cloud A/S' control	REVI-IT's test	Test results
8.2.1	*Classification* Information is classified in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification.	We have inspected the policy for classification of information.	No deviations noted.
8.2.2	*Labelling of information* An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inquired about the procedures for labelling of data and we have inquired about information that is labelled in accordance with the classification system.	No deviations noted.
8.2.3	*Handling of assets* Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inquired about procedures for handling of assets and we have inspected the procedures.	No deviations noted.

A.8.3 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
8.3.1	*Management of removable media* Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	We have inquired about managing portable media and we have inspected documentation for the solution.	No deviations noted.
8.3.2	*Disposal of media* Media are being disposed of securely when no longer required using formal procedures.	We have inquired about media disposal guidelines.	No deviations noted.
8.3.3	*Physical media in transit* Media containing information are protected against unauthorized access misuse or corruption during transportation.	We have inspected procedures for protection of media during transportation.	No deviations noted.

A.9 Access control

A.9.1 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
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inquired into the policy of managing access control in order to establish whether it is updated and approved.	No deviations noted.
9.1.2	*Access to network and network services.* Users are only being provided with access to the network and network services that they have been specifically authorized to use.	We have inquired about managing access to networks and network services, and we have inspected the solution. We have inspected a number of users, to establish that they only have access to approved networks and services, based on work-related requirements.	No deviations noted.

A.9.2 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
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inquired into the procedure for creating and aborting users and we have inspected the procedures. We have inspected a sample of documentation for user creation and removal of users.	No deviations noted.
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services	We have inquired that a procedure for user administration has been established. We have inspected that the procedure for user administration has been implemented.	No deviations noted.

No.	any.cloud A/S' control	REVI-IT's test	Test results
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inquired about procedures for granting rights, use and limitation of privileged access rights. We have inspected a sample of privileged users to establish whether the procedure has been followed.	No deviations noted.
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have inspected the procedure regarding allocation of access codes to platforms.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals	We have inquired into the process of periodic review of users and we have inspected checks for review. We have inquired into the procedure for the incorporation of rights and we have inspected the procedure.	No deviations noted.
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have inspected a sample of resigned employees and we have inspected whether their access rights have been cancelled.	No deviations noted.

A.9.3 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
9.3.1	*Use of secret authentication information.* Users are required to follow the organizations' s practices in the use of secret authentication information.	We have inspected the guidelines for use of secret authentication information.	No deviations noted.

A.9.4 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
9.4.1	*Information access restriction* Access to information and application system functions has been restricted in accordance with the access control policy.	We have inspected guidelines and procedures for securing access restriction to application system functions.	No deviations noted.
9.4.2	*Secure log-on procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inquired about procedure for secure log-on and we have inspected the implemented procedure.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inquired that policies and procedures requires quality passwords We have inquired that systems for administration of access codes are configured in accordance with the requirements.	No deviations noted.
9.4.4	*Use of privileged utility programs* The use of utility programs that might be capable of overriding system and application controls have been restricted and tightly controlled.	We have inquired into procedures to protect against bypassing of system- and application controls by using privileged utility programs.	No deviations noted.

A.10 Cryptography

A.10.1 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
10.1.1	Policy on the use of cryptographic controls A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inquired into the policy of using encryption, and we have on a sample basis inspected the use of cryptography.	No deviations noted.
10.1.2	*Key Management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, that supports the company use of cryptographic techniques.	No deviations noted.

A.11 Physical and environmental security

A.11.1 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
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inquired into the procedure for physical security of facilities and security perimeters. We have inquired into relevant locations and their security perimeter, to establish whether security measures have been implemented to prevent unauthorized access.	No deviations noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inquired into the procedures for access control to secure areas. We have inquired about access points to establish whether personal access cards are used to gain access to production facilities.	No deviations noted.
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inquired about whether physical security has been applied to protect offices, rooms, and facilities. We have inspected, that an inspection of fire-fighting equipment, UPS installations etc. is performed. We have inspected that a test of generators, UPS installations etc. is performed.	No deviations noted.
11.1.4	*Protection against external and environmental threats.* Physical protection against natural disasters, malicious attack or accidents has been designed and applied.	We have inspected procedures for protection against external and environmental threats. We have inquired about implementation of security measures, to prevent threats from fire, heat and water and we have inspected relevant locations to make sure that fire-fighting equipment, fire-and smoke alarms, blocking of waterpipes, raised floors and alarms for testing of moisture, water etc. has been installed.	No deviations noted.

A.11.2 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**
11.2.1	*Equipment sitting and protection* Equipment is sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.	We have inquired into the procedure concerning sitting and protection of equipment.	No deviations noted.
11.2.2	*Supporting utilities (security of supply)* Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	We have inspected procedures for protection of equipment from power failure and other disruptions caused by failures in supporting utilities. We have inspected that backup power, UPS- installation and diesel generators, with adequate capacity is available.	No deviations noted.
11.2.3	*Cabling security* Power and telecommunications cabling carrying data or supporting information services are being protected from interception	We have inquired about the protection of selected power and telecommunications cabling to establish whether the cables are protected from interception.	No deviations noted.
11.2.4	*Equipment maintenance.* Equipment is being correctly maintained to ensure its continued availability and integrity.	We have inspected the procedure for maintenance of equipment to determine whether the procedure is adequate. We have inspected guidelines for maintenance of equipment.	No deviations noted.
11.2.5	*Removal of assets* Equipment information or software is not taken off-site without prior authorization.	We have inquired into guidelines for removal of equipment, information, and software from the company.	No deviations noted.

No.	any.cloud A/S' control	REVI-IT's test	Test results
11.2.6	*Security of equipment and assets off-premises.* Security has been applied to off-site assets considering the different risks of working outside the organization's premises.	We have inquired about securing of equipment and assets outside the company's premises.	No deviations noted.
11.2.7	*Secure disposal or re-use of equipment* All items of equipment containing storage media have been verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.	We have inquired into the procedure for deletion of data and software on storage media, before disposing of same.	No deviations noted.
11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	We have inquired into the procedure for protection of unattended equipment.	No deviations noted.
11.2.9	*Clear desk and clear screen policy.* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.	We have inquired into the policy of tidy desk and clear screen.	No deviations noted.

A.12 Operations security

A.12.1 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
12.1.1	*Documented operating procedures.* Operating procedures have been documented and made available to all users.	We have inquired about requirements for documentation and maintenance of operating procedures. We have inquired that documentation for operating procedures is accessible to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organization business processes information processing facilities and systems that affect information security have been controlled.	We have inquired about the procedure regarding changes of information handling equipment and -systems. We have inquired whether a selection of changes, made on platforms, databases and network equipment have been approved, tested, documented, and implemented in the production environment, according to the Change Management procedure.	No deviations noted.
12.1.3	*Capacity management* The use of recourses is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inquired into the procedure for monitoring use of recourses and adjustments of capacity, to ensure future capacity requirements. We have inspected that relevant platforms are included in the capacity requirement procedure.	No deviations noted.
12.1.4	*Separation of development-, test- and operations facilities.* Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.	We have inquired into securing the separation of development-, test- and operations facilities. We have on a sample basis inspected, that development, test, and production are either physically or logically separated.	No deviations noted.

A 12.2 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
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inquired into measures against malware. We have inquired about the use of antivirus software and we have inspected documentation for its use.	No deviations noted.

A.12.3 Backup
Control objective: To protect against loss of data

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.3.1	*Information backup* Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inquired into configuration of backup and we have inspected samples of documentation for the setup according to requirements. We have inspected that backup is monitored. We have inquired about testing of backupfile recovery and we have inspected documentation for recovery test.	No deviations noted.

A.12.4 Logging and monitoring
Control objective: To record events and generate evidence

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events have been produced, kept, and regularly reviewed.	We have inquired into user activity logging. We have inspected samples of logging configurations.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inquired about secure log information and we have inspected the solution. We have inquired into logging configurations to establish whether login information is protected against manipulation and unauthorized access.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged, and the logs protected and regularly reviewed.	We have inquired into procedures regarding logging of activities performed by system administrators and operators. We have inquired about database systems, to establish whether the actions of system administrators and operators are logged.	No deviations noted.
12.4.4	*Clock synchronization* The clocks of all relevant information processing systems within an organization or security domain have been synchronised to a single reference time source.	We have inquired into procedures for synchronization against a reassuring time server and we have inspected the solution.	No deviations noted.

A.12.5 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
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inquired about software installation guidelines on operating systems and we have - on a sample basis - inspected that the guidelines are followed.	No deviations noted.

A.12.6 Technical vulnerability management
Control objective: To prevent exploitation of technical vulnerabilities

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inquired into the procedure regarding gathering and evaluation of technical vulnerabilities. We have on a sample basis inspected servers, database systems and network component to establish, whether they are patched in time.	No deviations noted.
12.6.2	*Restriction on software installation* Rules governing the installation of software by users have been established and implemented.	We have inquired into restriction of user executed software installations	No deviations noted.

A.12.7 Information system audit consicerations
Control objective: To minimize the effect of audit activities on operational systems

No.	any.cloud A/S' control	REVI-IT's test	Test results
12.7.1	*Information system audit controls* Audit requirements and activities involving verification of operational systems are being carefully planned and agreed to minimize disruptions to business processes.	We have inquired about controls in connection with audit of information systems.	No deviations noted.

A.13 Communications security

A.13.1 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
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inquired into whether requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined. We have inspected documentation for network design and a range of security setups of network components.	No deviations noted.
13.1.2	*Security of network services* Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced.	We have observed that written requirements about security mechanisms, service levels and management requirements of all network services are present.	No deviations noted.

No.	any.cloud A/S' control	REVI-IT's test	Test results
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inquired into the guidelines for segregation of networks. We have inspected a range of accesses made between network zones to establish whether they are limited to essential services.	No deviations noted.

A.13.2 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
13.2.1	*Information transfer policies and procedures* Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.	We have inquired about data transfer policies and procedures.	No deviations noted.
13.2.2	*Agreements on information transfer* Agreements address the secure transfer of business information between the organization and external parties.	We have inquired about data transfer agreements.	No deviations noted.
13.2.3	*Electronic messaging* Information involved in electronic messaging is appropriately protected.	We have inquired about guidelines for electronic messaging of confidential information.	No deviations noted.
13.2.4	*Confidentiality or non-disclosure-agreements* Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information, are identified, and documented on a regular basis.	We have inquired about the procedure for establishing non-disclosure-agreements. We have inspected a signed non-disclosure-agreements to establish whether the procedure has been followed when hiring of new staff and closing of agreements with consultants.	No deviations noted.

A.15 Supplier relationships

A.15.1 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
15.1.1	*Information security policy for supplier relationships* Information security requirements for mitigating the risks associated with supplier's access to the organization's assets have been agreed with the supplier and documented.	We have inquired about the procedure for closing agreements with subcontractors. We have inspected the procedure regarding selection and protection of test data.	No deviations noted.
15.1.2	*Addressing security within supplier agreements* All relevant information security requirements are established and agreed with each supplier that may access process store communicate or provide IT infrastructure components for the company's information.	We have inquired about the procedure for conclusion of contract with subcontractors.	No deviations noted.
15.1.3	*Information and communication technology supply chain* Agreements with suppliers are including requirements to address the information security risks associated with information and communications technology services and product supply chain.	We have inquired about contract requirements for subcontractors in relation to information and communication technology supply chain.	No deviations noted.

15.2 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
15.2.1	*Monitoring and review of third-party services* Organizations are regularly monitoring review and audit supplier service delivery.	We have inquired if the procedure for monitoring and review of services from subcontractors is according to the contract. We have inspected an operations report, that are used to ensure that services rendered are according to the contract. Vi have inspected that review and evaluation of relevant audit reports about subcontractors, have been performed.	No deviations noted.
15.2.2	*Manage changes to the third-party services* Changes in supplier services, including maintenance and improvement of existing information security policies, procedures, and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have inquired about management of changes with the subcontractor and we have inspected the documentation for handling this.	No deviations noted.

A.16 Information security incident management

A.16.1 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
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities. In addition, we have inspected the procedure for handling information security incidents.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines.	No deviations noted.
16.1.3	*Reporting security weaknesses* Employees and contractors using the organization's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inquired about information security events during the period and we have inspected these.	No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inquired into the procedure for assessment, response and evaluation of information security breaches.	No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have on a sample basis inspected that information security incidents have been responded to, in accordance with the documented procedures.	No deviations noted.

No.	any.cloud A/S' control	REVI-IT's test	Test results
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about Problem-Management function which analyses information security incidents to reduce probability of recurrence.	No deviations noted.
16.1.7	*Collection of evidence* The organization has defined and applied procedures for the identification collection acquisition and preservation of information which can serve as evidence.	We have inquired about procedures for collection of evidence.	No deviations noted.

A.17 Information security aspects of business continuity management

A.17.1 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
17.1.1	*Planning information security continuity* The organization has determined its requirements for information security and the continuity of information security management in adverse situations e.g. during a crisis or disaster.	We have inquired about the preparation of a contingency plan to ensure the continuation of operations in the event of crashes and the like, and we have inspected the plan.	No deviations noted.
17.1.2	*Implementing information security continuity* The organization has established document implementation and maintenance of processes procedures and controls to ensure the required level of continuity for information security during an adverse situation.	We have inquired about procedures to ensure that all relevant systems are included in the contingency plan and we have inspected that the contingency plan is properly maintained.	No deviations noted.

No.	any.cloud A/S' control	REVI-IT's test	Test results
17.1.3	*Verify review and evaluate information security continuity* The organization is verifying the established and implemented information security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.	We have inquired about test of the contingency plan and we have inspected documentation for tests performed. We have also inquired into reassessment of the contingency plan, and we have inspected documentation for reassessment.	No deviations noted.

A.17.2 Redundancies
Control objective: To ensure availability of information processing facilities

No.	any.cloud A/S' control	REVI-IT's test	Test results
17.2.1	*Availability of information security processing facilities* Information processing facilities have been implemented with redundancy sufficient to meet availability requirements.	We have inquired about the availability of operating systems and we have inspected the established measures.	No deviations noted.

A.18 Compliance

A.18.2 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
18.2.1	*Independent review of information security* Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have observed, that independent evaluation of information security has been established.	No deviations noted.
18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inquired for management's procedures for compliance with security policies and security standards.	No deviations noted.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have inquired for internal controls to ensure compliance with security policies and procedures, and we have inspected selected controls.	No deviations noted.