



revi-it

Building a safer society through compliance

Assurance report

Zentura A/S

ISAE 3402 type 2 assurance report on general it-controls for the period 1 November 2020 to 30 October 2021 related to operating of hosting-platform

December 2021

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

Table of contents

Section 1:	Description of Zentura A/S' services in connection with operating of hosting-platform, and related general it-controls	1
Section 2:	Zentura A/S' statement.....	10
Section 3:	Independent service auditor's assurance report on the description of controls, their design and functionality	11
Section 4:	Control objectives, controls, and service auditor testing	14

Section 1: Description of Zentura A/S' services in connection with operating of hosting-platform, and related general it-controls

The following is a description of Zentura A/S' services which are included in the general it-controls of this assurance report. The report includes general processes and system setups etcetera with Zentura A/S. Processes and system setups etcetera, individually agreed with Zentura 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.

IT Control Description 2021

Description of Zentura A/S' controls in connection with sales and operation of hosting platform.

Document Approval History

Document history			
Version	Date and year	Change	Changed by
1.0	1 June 2015		AFH
2.0	14 June 2016		AFH
3.0	8 August 2017		CLJ / AFH
3.1	9 October 2017		CLJ
3.2	5 July 2018	Updating of patch process	CLJ
3.3	12 March 2019	Control description of the "minimum goals for good hosting" in relation to the handling of redundant internet connection and the fight against cybercrime added.	CLJ
3.4	5 May 2019	Control description updated in connection with moving to a new office in Taastrup.	CLJ
3.5	9 May 2020	Review of control description and minor corrections.	CLJ

Introduction

In the company, we have implemented a number of controls, which is needed to ensure quality and document quality in our services. All controls, whether related to a procedural or technical handling, have an executive responsible, and in some cases also a responsible approver.

Our controls are aimed at both specific work actions and processes for a number of work actions, which may also have specific controls associated with further. Specific work actions are described in Standard Operation Procedure documents (SOPs).

Timing for a given control is always given over a period of time, even if a given control often had to be practically performed in a particular month year after year.

Scope

We specialize in consulting, implementation, operation, and maintenance of business-critical IT solutions, and we offer our customers different types of hosting. We have a special focus and competencies within consulting, setup, upgrading, operation, and maintenance of Citrix and Nutanix solutions. We put quality and reliability first, and since the vast majority of our products and services are delivered in real time, we naturally have 24/7/365 customer service, monitoring and promise 99.9% availability.

To guarantee our services, we regularly maintain our systems, our competencies, and our documentation.

We are our customers' IT department and handle all aspects related to this.

4. Risk assessment and management

Registration, assessment, mitigation, and risk evaluation are an integral part of all our business processes. Quality and reliability are of the utmost importance to us, and to our customers, which is why we continuously take a position on all matters that may relate to the quality of our services and our business in general. All with due regard for our surroundings and the eternally fluctuating threat picture.

All threats are assessed systematically and uniformly, and to ensure transparency, clarity, and documentation, the established classification method is used. Identification, analysis, and assessment of risks of significance to our business can be based on both external threats as well as internal conditions.

The risk analysis is management approved and is reviewed at least once a year.

5. Information security policies

5.1 Guidelines for managing information security

In our IT security policy, we have described how we ensure information security in our business. Our IT security policy cannot be deviated from, either for customers, employees, or suppliers, and it is the company's management that approves guidelines and makes the necessary updates of the same.

The company's IT security policy is updated if changes are made or new business areas are implemented, and the policy is reviewed in its entirety at least once a year.

6. Organization of information security

6.1 Internal organization

Once we have changed the IT security policy, and at least after the annual review, the changes will be presented internally at the next monthly meeting for the staff. Likewise, external suppliers etcetera involved and informed if relevant. The company's CEO and partner are responsible for the company's information security.

6.2 Mobile equipment (data-bearing media) and remote workstations

We have no data-bearing media, except server room media and mobile phones. We only have access to mail, calendar, and contacts via our mobile phones, just as we have connected a number of security policies. We do not use local media such as USB sticks for data storage. The mobile equipment policy is part of Zentura's security policy.

7. Human recourse security

7.1 Prior to employment

Prior to hiring employees, a hiring procedure is followed. It is the hiring employee / partner who is responsible for the HR related controls. For consultants who must have access to (parts of) our network, a task-specific contract is always prepared, a dedicated declaration of confidentiality is obtained, and other relevant documentation is obtained. It is the COO who is responsible for ensuring that all HR processes and procedures are complied with, and considering the size of the company, these tasks are typically handled by the COO. The technical creation of employees - as well as consultants, is done according to relevant SOPs. We also have a process for controlling all users with rights to the corporate network.

7.2 During employment

Employees, and external parties when relevant, are trained and trained in our guidelines for IT security and the tasks derived therefrom. This takes place as peer training, at office meetings and the like. We also have a procedure for training / education / certification of employees.

Dependence on key employees

Through our documentation and descriptions, we secure ourselves against personal dependence, just as we work with double roles in all functions to the greatest possible extent.

7.3 Termination or change of employment

The technical settlement of employees - as well as consultants, is carried out in accordance with relevant SOPs. We also have a process for controlling all users with rights to the corporate network.

8. Asset management

8.1 Responsibility for assets

All assets are owned by the company and there are records of the same.

8.2 Classification of information

All company data, both own data and customer data, enjoys the same protection. There may be special conditions agreed for certain customers, and these conditions will be regulated and handled by special agreement.

8.3 Media handling

We have no data-bearing media, except server room media and mobile phones. All mobile phones are secured with security policies, including connection authentication per device. We do not use local media such as USB sticks.

9. Access control

9.1 Business requirements of access control

Our customers' users are created, changed, and dismantled on the basis of requirements from our customers. Internal users are created on the basis of written request from management. All users are personally identifiable. Service accounts that are only used systematically, the option for actual logon is deactivated. All users, customer users as well as internal users, have password restrictions. Internal users and their access level are periodically reviewed by management. All employees are created with differentiated access, and thus only have access to the systems and data that are relevant to their respective job functions. We also use 2-factor authentication, which is mandatory, also for customers.

9.2 User access management

Onboarding of new customers is done according to established procedures and relevant SOPs. A representative from our Sales and Management approves the customer setup, which is why compliance with the contract, technology and business requirements is ensured. Each customer contract also contains a specification of who, at the customer's, has the rights to submit and / or approve IT change requests on behalf of the company in question to Zentura, so that there is never any doubt about who is responsible for an action / change performed.

9.3 User responsibilities

Administration of user access is performed according to established procedures and relevant SOPs. Guidelines for user responsibility are available in the company's IT security policy and employee handbook.

9.4 System and application access control

Administration of system and application accesses is performed according to established procedures and SOPs.

10. Cryptography

10.1 Cryptographic controls

All network communication between us and our customers is protected by encryption. Access to, and administration of, encryption keys is handled solely by the company's management. All traffic to and from Zentura's network is protected by SSL certificates trusted by Trustzone.

11. Physical and environmental security

11.2 Equipment

Disposal of media

We own all server room media. Media is destroyed as part of our purchasing agreement with the supplier. In case of theft of mobile phone, remote deletion of the phone is done. It will then not be possible to access mail and calendar data from the phone.

Secure areas

Business Cloud

The Business Cloud 365 solution is located in Microsoft Azure sites in Netherlands and Ireland. These areas have a higher degree of protection than the Danish datacentres.

Zentura has no equipment in the Microsoft Azure datacentres. Everything is virtual from a customer perspective. Disposal of virtual equipment is only a matter of deleting the virtual equipment from the Azure datacentres.

12. Operations security

12.1 Operational procedures and responsibilities

Our documentation and work processes help to ensure a stable, correct, and reliable service, where personal dependence and 'sludge errors' are minimized. Changes to the systems follow our ITIL Change Management process, whereby they must be approved by our "Change Advisory Board" before implementation.

12.1.3 Capacity management

Availability is one of our core values, and we take pride in always delivering the expected quality of service to our customers. We monitor our capacity, both disks, CPU and traffic, and we can continuously, and without inconvenience to customers, expand our capacity.

12.2 Protection from malware

We consider malware to be one of the biggest threats to our business, and our technical measures ensure the highest possible level of security that malware cannot be settled in our environments. We minimize the risk both in terms of perimeter safety, but also damage delimitation, should an unintended event occur. We also have a definite contingency, should an unintended event require the implementation of extraordinary measures.

Zentura follows all the industry association's recommendations regarding combating cybercrime. See section 18.2.

12.3 Backup

On Zentura's hosting platform, snapshot backups are made every night. This means that a full copy of all data is made, server system files, user data, file services, databases, and all other data. A snapshot is a complete copy of the server the moment the snapshot is taken - with no data loss at all. After each snapshot, a copy of the snapshot is copied to the opposite data centre. These snapshots are stored for 4 days on the primary site so that the restore can be performed without prior copying from the secondary data centre. All snapshots are stored for 30 days on the secondary data centre. This policy is used on both Zentura's and customers' servers and data.

On Azure services all data (mail, OneDrive, SharePoint, teams, ...) is backed up for 30 days using a backup service provider.

On customers with their own infrastructure, the customer's own backup system is used for backup and the customer's own policy is followed.

12.4 Logging and monitoring

Our technical set-up focuses on the same values, and protection against unauthorized access to our data is of the highest priority. We have systems for monitoring and securing networks and Internet use, and all emails (incoming and outgoing) are scanned for viruses by an external provider. We monitor our systems daily via automated systems for measuring limit values.

Alarming, if a critical incident is found, is sent to our operations staff and outside office hours to our operations guard. Events for login and logout on our platforms are logged, and we only use personally identifiable user accounts, so it is possible to identify which people have been logged on.

12.5 Control of operational software

Patching of VM's in our datacentre is done weekly in a defined service window. The service window is stated in the company's general terms and conditions and does not need to be notified separately. For example, all critical Microsoft system updates, Windows security updates classified as "Critical" and "Security Updates," are automatically installed in the agreed service window. A number of third-party programs such as Java, Adobe Reader, etcetera are updated along with various Microsoft patches.

Patching of Azure VM's is done with Microsoft Automation in the same service windows as VM's in our own datacentres.

All "Critical" and "Security" patches are installed within 2 months of release.

12.6 Technical vulnerability management

Our systems are protected against uncontrolled software installation. Our customers are also shielded from the possibility of installing software.

Our Service Desk receives on a regular basis mail from CSIS Platinum Alert Service about vulnerabilities. All alerts are handled in the Service Desk by today's guard and checked if the vulnerability is relevant for Zentura.

12.7 Information system audit considerations

We prioritize internal audits on an ongoing basis, including internal random checks, and the responsibility is rooted in our operations manager. The time for performing the annual external audit is planned in collaboration with our auditors.

13. Communications security

13.1 Network security management

All approved network traffic (incoming) comes through our firewall, and we have VPN / MPLS connections to all customers. We have a fixed procedure for documentation of internal network, logical division of networks, naming of devices, etcetera. Access to the company's services via mobile devices is not permitted, however, access to mail, calendar and address book is permitted. To have this access, a number of security policies are imposed on the phone, which is an integral part of our device setup process. All standard changes have a dedicated SOP. All significant changes are discussed, prioritized, and approved by management.

13.2 Information transfer

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

14. Acquisition, development, and maintenance of systems

14.1 Security requirements of information systems

Information security-related requirements are part of our processes, and changes / new purchases are always assessed from a security perspective, cf. our risk analysis.

14.2 Security, development- and supporting processes

All changes to systems are handled via change procedure.

14.3 Test data

Test data must never be personal or confidential data. Test data enjoys the same protection as all other data.

15. Supplier relationships

15.1 Information security in supplier relationships

All our supplier and partner agreements contain regulation of confidentiality.

15.2. Supplier service delivery management

We have a process to ensure that our supplier agreements contain relevant security matters, such as matters of monitoring, confidentiality, intellectual property rights and delivery security. Auditor's statement (s) are also obtained from our critical suppliers.

16: Information security incident management

16.1 Management of information security incidents and improvements

We define security incidents broadly and have procedures for handling these incidents. We have established a number of measures to prevent the safety incidents from occurring, and in addition we have operational monitoring with on-call arrangements, with which we can react immediately should an unintended incident occur. We receive daily security information from CSIS, and we have Secure DNS, which helps us stay ahead. We also stay professionally updated using the manufacturers' websites, discussion forums, etcetera.

16.16 Learning from information security incidents

All security breaches are documented for internal use, and the incident is reviewed with all relevant employees at the earliest opportunity. Depending on the nature of the incident, new processes and procedures are developed so that we avoid the incident occurring again. Security-related topics, general as well as current topics, are also reviewed at internal meetings. In criminal cases, a police investigation takes place, where our logging and other monitoring can be used to clarify and evaluate the security incident.

17. Information security aspects of business continuity management

17.1. Information security continuity

An risk analysis has been established, which lists the possible scenarios that may affect the operation of our systems, and contingency plans has been established that describes how the operation should re-established after crash.

Units in the data centres can be re-established within 3 days. In most cases, however, it will happen on the same day, as we have 4 hours of service / replacement on all hardware.

17.2 Redundancies

We use two separate data centres, and should a data centre become inaccessible, we can switch to the secondary site.

We have redundant internet connections to the primary data centre, as well as MPLS to the secondary, which is why we have another internet connection that will be able to route traffic through, if both internet connections in the primary data centre are down. Zentura hereby complies with the industry association's recommendations regarding good hosting.

18. Compliance

Compliance with statutory and contractual requirements

We are not subject to special legislation in relation to our services. However, our customers may be subject to special legislation, and wherever this may be the case, our support is agreed separately.

Data Processor Agreements

We have data processor agreements with all our customers.

Contingency

Should an emergency arise, Zentura has prepared a contingency plan. The contingency plan has been prepared in accordance with and in accordance with our IT security policy and our risk analysis, and it is maintained at least annually. The plan is tested, and both the plan and procedures are anchored in our operational documentation and procedures. Our contingency planning considers that we can deliver our services on time at any time - almost no matter what happens.

18.2 Review of information security

We are audited annually by an external auditor to obtain a statement without reservation for compliance with the controls mentioned in this description. We follow the framework within ISO 27002, which the aforementioned auditor certifies in an ISAE3402-II statement.

Complementary controls

Unless otherwise agreed, our customers are responsible for connecting to our servers. In addition, our customers are responsible for, unless otherwise agreed, that; i) The agreed level of backup covers the customer's needs, ii) User administration, including requests for creation and downsizing of user, and periodic review, of the customer's own users, iii) That traceability is maintained in third party software that the customer manages, iv) That customer specific software solutions support the backup technology offered by us, v) Special agreement for backup jobs that require encryption password, where the customer is solely responsible for handling and storing the encryption password, and vi) Request for access to the customer's server environment for the customer's third party suppliers, vii) Customer's notification to the Data Inspectorate, for whom this may be relevant.

This is a fixed part of the agreement basis with the customer.

Changes in the period

Zentura has developed a new concept for a Business Cloud 365, based on Microsoft Azure's services.

Section 2: Zentura A/S' statement

The accompanying description has been prepared for customers who have used Zentura A/S' 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.

Zentura A/S is using subservice organisations Interxion and Microsoft. This assurance report is prepared in accordance with the carve-out method and Zentura A/S' description does not include control objectives and controls within Interxion and Microsoft.

Zentura A/S confirms that:


- (a) The accompanying description in Section 1 fairly presents the general it-controls related to Zentura A/S' hosting platform, processing customer transactions for the period 1 November 2020 to 30 October 2021

The 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, by which those transactions are initiated
 - 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 November 2020 to 30 October 2021
- (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 November 2020 to 30 October 2021. 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 November 2020 to 30 October 2021

Taastrup, den 7 December 2021

Zentura A/S


Christian Pedersen
CEO

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

To Zentura A/S, their customers, and their auditors.

Scope

We have been engaged to report on Zentura A/S' description in Section 1 of its system for delivery of Zentura A/S' Services throughout the period 1 November 2020 to 30 October 2021 (the description) and on the design and operation of controls related to the control objectives stated in the description.

Zentura A/S is using subservice organisations Interxion and Microsoft. This assurance report is prepared in accordance with the carve-out method and Zentura A/S' description does not include control objectives and controls within Interxion and Microsoft.

Some of the control objectives stated in Zentura 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 Zentura A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Zentura A/S' responsibility

Zentura 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, Zentura 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 1¹ 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 Zentura 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

Zentura 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 Zentura 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 01 November 2020 to 30 October 2021, 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 November 2020 to 30 October 2021 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 November 2020 to 30 October 2021.

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 Zentura 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, 7 December 2021

REVI-IT A/S
State authorised public accounting firm



Henrik Paaske
State authorised public accountant



Basel Rimon Obari
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 Zentura A/S' subservice organisations.

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

4.2. Tests

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

Method	General description
Inquiries	Interview with appropriate personnel at Zentura 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 in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals.
Re-performance	Re-performance of controls in order 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 Zentura A/S.

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.	Zentura A/S' control	REVI-IT's test	Test results
5.1.1	<p><i>Policies for information security</i></p> <p>A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.</p>	<p>We have inspected the information security policy and we have inspected documentation for management approval of the information security policy.</p>	<p>No deviations noted.</p>
5.1.2	<p><i>Review of policies for information security</i></p> <p>The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.</p>	<p>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.</p>	<p>No deviations noted.</p>

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 organisation

No.	Zentura A/S' control	REVI-IT's test	Test results
6.1.1	<p><i>Information security roles and responsibilities.</i></p> <p>All information security responsibilities are defined and allocated.</p>	<p>We have inspected the organisation chart.</p> <p>We have inspected the guidelines for information security roles and responsibilities.</p>	No deviations noted.
6.1.2	<p><i>Segregation of duties.</i></p> <p>Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.</p>	<p>We have inspected procedures regarding granting and maintenance of segregation of duties and functions.</p> <p>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, and whether developers have access to the production environment.</p>	No deviations noted.
6.1.4	<p><i>Contact with special interest groups</i></p> <p>Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.</p>	We have inspected the procedure regarding maintenance of rules for appropriate contact with special interest groups, security fora and professional organisations.	No deviations noted.

A.6.2 Mobile devices and teleworking

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

No.	Zentura A/S' control	REVI-IT's test	Test results
6.2.1	<p><i>Mobile device policy</i></p> <p>Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.</p>	<p>We have inspected the policy for securing of mobile devices.</p> <p>We have inspected, that technical controls for securing of mobile devices have been defined.</p> <p>We have – by sample test– inspected that technical controls are implemented on mobile devices.</p>	No deviations noted.
6.2.2	<p><i>Teleworking</i></p> <p>Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.</p>	<p>We have inspected the policy to secure teleworking, and we have inspected the underlying security measures for protection of remote workspaces.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
7.1.1	<p><i>Screening</i></p> <p>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.</p>	<p>We have inquired into the procedure for employment of new employees and the security measures needed in the process.</p> <p>We have inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.</p>	No deviations noted.
7.1.2	<p><i>Terms and conditions of employment</i></p> <p>The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security.</p>	<p>We have inspected a selection of contracts with employees and consultants in order to determine whether these are signed by the employees.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
7.2.1	<p><i>Management responsibility</i></p> <p>Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.</p>	<p>We have inquired about procedure concerning establishing requirements for employees and partners.</p> <p>We have inquired whether it is required by management that employees observe the IT-security policy</p>	No deviations noted.
7.2.2	<p><i>Information security awareness education and training</i></p> <p>All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.</p>	<p>We have inquired about procedures to secure adequate training and education (awareness training).</p> <p>We have inspected documentation for activities developing and maintaining security awareness with employees.</p>	No deviations noted.
7.2.3	<p><i>Disciplinary process</i></p> <p>There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.</p>	<p>We have inspected the sanctioning guidelines and we have inspected that the guidelines have been communicated.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
7.3.1	<p><i>Termination or change of employment responsibility</i></p> <p>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.</p>	<p>We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment.</p> <p>We have inspected documentation, that information security has been defined and communicated.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
8.1.1	<p><i>Inventory of assets</i></p> <p>Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.</p>	We have inspected asset listings.	No deviations noted.
8.1.2	<p><i>Ownership of assets</i></p> <p>Assets maintained in the inventory are being owned.</p>	We have inspected record of asset ownership.	No deviations noted.
8.1.3	<p><i>Acceptable use of assets</i></p> <p>Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.</p>	We have inquired about the guidelines for the use of assets and we have inspected the guidelines.	No deviations noted.
8.1.4	<p><i>Return of assets</i></p> <p>All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.</p>	We have inquired into the procedure for securing the return of assets delivered, and we have inspected the procedure.	No deviations noted.

A.8.3 Media handling

Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media

No.	Zentura A/S' control	REVI-IT's test	Test results
8.3.1	<p><i>Management of removable media</i></p> <p>Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.</p>	<p>We have inquired about managing portable media and we have inspected documentation for the solution.</p>	No deviations noted.
8.3.2	<p><i>Disposal of media</i></p> <p>Media are being disposed of securely when no longer required using formal procedures.</p>	<p>We have inquired about media disposal guidelines.</p> <p>We have inspected that media are disposed of, according to procedures.</p>	No deviations noted.
8.3.3	<p><i>Physical media in transit</i></p> <p>Media containing information are protected against unauthorised access misuse or corruption during transportation.</p>	<p>We have inspected procedures for protection of media during transportation.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
9.1.1	<p><i>Access control policy</i></p> <p>An access control policy has been established, documented, and reviewed based on business and information security requirements.</p>	<p>We have inquired into the policy of managing access control in order to establish whether it is updated and approved.</p>	No deviations noted.
9.1.2	<p><i>Access to network and network services.</i></p> <p>Users are only being provided with access to the network and network services that they have been specifically authorized to use.</p>	<p>We have inquired about managing access to networks and network services, and we have inspected the solution.</p> <p>We have inspected a number of users, in order to establish that they only have access to approved networks and services, based on work-related requirements.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
9.2.1	<p><i>User Registration and de-registration</i></p> <p>A formal user registration and de-registration process has been implemented to enable assignment of access rights.</p>	<p>We have inquired into the procedure for creating and aborting users and we have inspected the procedures.</p> <p>We have inspected a sample of documentation for user creation and removal of users.</p>	No deviations noted.
9.2.2	<p><i>User access provisioning</i></p> <p>A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services</p>	<p>We have inquired into whether a procedure for user administration has been established.</p> <p>We have inspected that the procedure for user administration has been implemented.</p>	No deviations noted.
9.2.3	<p><i>Management of privileged access rights</i></p> <p>The allocation and use of privileged access rights have been restricted and controlled.</p>	<p>We have inquired about procedures for granting rights, use and limitation of privileged access rights.</p> <p>We have inspected a sample of privileged users to establish whether the procedure has been followed.</p>	No deviations noted.
9.2.4	<p><i>Management of secret-authentication information of users</i></p> <p>The allocation of secret authentication information is controlled through a formal management process.</p>	<p>We have inspected the procedure regarding allocation of access codes to platforms.</p> <p>We have for a number of allocations inspected, that the procedure is followed.</p>	No deviations noted.
9.2.5	<p><i>Review of user access rights</i></p> <p>Asset owners are reviewing user's access rights at regular intervals</p>	<p>We have inquired into the process of periodic review of users and we have inspected checks for review.</p> <p>We have inquired into the procedure for the incorporation of rights and we have inspected the procedure.</p>	No deviations noted.
9.2.6	<p><i>Removal or adjustment of access rights</i></p> <p>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.</p>	<p>We have inquired into procedures about discontinuation and adjustment of access rights.</p> <p>We have inspected a sample of terminated employees and we have inspected whether their access rights have been cancelled.</p>	No deviations noted.

A.9.3 User responsibilities

Control objective: To make users accountable for safeguarding their authentication information

No.	Zentura A/S' control	REVI-IT's test	Test results
9.3.1	<p><i>Use of secret authentication information</i></p> <p>Users are required to follow the organisations' s practices in the use of secret authentication information.</p>	<p>We have inspected the guidelines for use of secret authentication information.</p>	<p>No deviations noted.</p>

A.9.4 System and application access control

Control objective: To prevent unauthorised access to systems and applications

No.	Zentura A/S' control	REVI-IT's test	Test results
9.4.2	<p><i>Secure log-on procedures</i></p> <p>Access to systems and applications is controlled by procedure for secure logon.</p>	<p>We have inquired about procedure for secure log-on and we have inspected the implemented procedure.</p>	<p>No deviations noted.</p>
9.4.3	<p><i>Password management system</i></p> <p>Password management systems are interactive and have ensured quality passwords.</p>	<p>We have inquired into whether policies and procedures require quality passwords</p> <p>We have inquired into whether systems for administration of access codes are configured in accordance with the requirements.</p>	<p>No deviations noted.</p>

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.	Zentura A/S' control	REVI-IT's test	Test results
10.1.1	<p>Policy on the use of cryptographic controls</p> <p>A policy for the use of cryptographic controls for protection of information has been developed and implemented.</p>	<p>We have inquired into the policy of using encryption, and we have on a sample basis inspected the use of cryptography.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
11.1.1	<p><i>Physical security perimeter</i></p> <p>Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.</p>	<p>We have inquired into the procedure for physical security of facilities and security perimeters.</p> <p>We have inquired into relevant locations and their security perimeter, in order to establish whether security measures have been implemented to prevent unauthorized access.</p>	No deviations noted.
11.1.2	<p><i>Physical entry control</i></p> <p>Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.</p>	<p>We have inquired into the procedures for access control to secure areas.</p> <p>We have inspected a sample of access points in order to establish whether personal access cards are used to gain access to production facilities.</p>	No deviations noted.

No.	Zentura A/S' control	REVI-IT's test	Test results
11.1.3	<p><i>Securing offices, rooms, and facilities</i></p> <p>Physical security for offices rooms and facilities has been designed and applied.</p>	<p>We have – by sample test – inspected that physical security has been applied to protect offices, rooms, and facilities.</p> <p>We have inspected, that an inspection of fire-fighting equipment, UPS installations etcetera is performed.</p> <p>We have inspected that a test of generators, UPS installations etcetera is performed.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
11.2.8	<p><i>Unattended user equipment</i></p> <p>Users are ensuring that unattended equipment has appropriate protection.</p>	We have inquired into the procedure for protection of unattended equipment.	No deviations noted.
11.2.9	<p><i>Clear desk and clear screen policy</i></p> <p>A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
12.1.1	<p><i>Documented operating procedures</i></p> <p>Operating procedures have been documented and made available to all users.</p>	<p>We have inquired about requirements for documentation and maintenance of operating procedures.</p> <p>We have inquired into whether documentation for operating procedures is accessible to relevant employees.</p>	No deviations noted.
12.1.2	<p><i>Change management</i></p> <p>Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.</p>	<p>We have inquired about the procedure regarding changes of information handling equipment and -systems.</p> <p>We have inquired into 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.</p> <p>We have inspected servers, database systems and network components, in order to find examples of actual changes made, and locate documentation that Change Management procedure has been followed.</p>	No deviations noted.
12.1.3	<p><i>Capacity management</i></p> <p>The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.</p>	<p>We have inquired into the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements.</p> <p>We have inspected that relevant platforms are included in the capacity requirement procedure.</p>	No deviations noted.
12.1.4	<p><i>Separation of development-, test- and operations facilities.</i></p> <p>Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.</p>	<p>We have inquired into securing the separation of development-, test- and operations facilities.</p> <p>We have – by sample test - inspected, that development, test, and production are either physically or logically separated.</p>	No deviations noted.

A.12.2 Protection from malware
Control objective: To ensure that information and information processing facilities are protected against malware

No.	Zentura A/S' control	REVI-IT's test	Test results
12.2.1	<p><i>Control against malware</i></p> <p>Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.</p>	<p>We have inquired into measures against malware.</p> <p>We have inquired about the use of antivirus software and we have inspected documentation for its use.</p>	No deviations noted.

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

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

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

No.	Zentura A/S' control	REVI-IT's test	Test results
12.4.1	<p><i>Event logging</i></p> <p>Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.</p>	<p>We have inquired into user activity logging.</p> <p>We have inspected samples of logging configurations.</p>	No deviations noted.

No.	Zentura A/S' control	REVI-IT's test	Test results
12.4.2	<p><i>Protection of log information</i></p> <p>Logging facilities and log information are being protected against tampering and unauthorized access.</p>	<p>We have inquired about secure log information and we have inspected the solution.</p> <p>We have inquired into a selection of logging configurations in order to establish whether login information is protected against manipulation and unauthorized access.</p>	No deviations noted.
12.4.3	<p><i>Administrator and operator logs</i></p> <p>System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.</p>	<p>We have inquired into procedures regarding logging of activities performed by system administrators and operators.</p> <p>We have inspected logon setups on chosen servers and database systems, in order to establish whether the actions of system administrators and operators are logged.</p>	No deviations noted.
12.4.4	<p><i>Clock synchronization</i></p> <p>The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.</p>	<p>We have inquired into procedures for synchronization against a reassuring time server and we have inspected the solution.</p>	No deviations noted.

A.12.5 Control of operational software

Control objective: To ensure the integrity of operational systems

No.	Zentura A/S' control	REVI-IT's test	Test results
12.5.1	<p><i>Installation of software on operational systems</i></p> <p>Procedures are implemented to control the installation of software on operational systems.</p>	<p>We have inquired about software installation guidelines on operating systems and we have on a sample basis inspected that the guidelines are followed.</p>	No deviations noted.

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

No.	Zentura A/S' control	REVI-IT's test	Test results
12.6.1	<p><i>Management of technical vulnerabilities</i></p> <p>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.</p>	<p>We have inquired into the procedure regarding gathering and evaluation of technical vulnerabilities.</p> <p>We have – by sample test - inspected servers, database systems and network components in order to establish, whether they are patched in time.</p>	No deviations noted.
12.6.2	<p><i>Restriction on software installation</i></p> <p>Rules governing the installation of software by users have been established and implemented.</p>	<p>We have inquired into restriction of user executed software installations.</p> <p>We have inspected, that regulations for software installations are followed.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
13.1.1	<p><i>Network controls</i></p> <p>Networks are managed and controlled to protect information in systems and applications.</p>	<p>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.</p> <p>We have inspected documentation for network design and a range of security setups of network components, in order to establish whether the defined rules and regulations have been implemented.</p>	No deviations noted.

No.	Zentura A/S' control	REVI-IT's test	Test results
13.1.2	<p><i>Security of network services</i></p> <p>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.</p>	<p>We have observed that written requirements about security mechanisms, service levels and management requirements of all network services are present.</p> <p>We have inspected a range of network components in order to estimate whether the components have been set up according to requirements and contractor's recommended baselines.</p>	No deviations noted.
13.1.3	<p><i>Segregation of networks</i></p> <p>Groups of information services users and information systems are segregated on networks.</p>	<p>We have inquired into the guidelines for segregation of networks.</p> <p>We have inspected a range of accesses made between network zones to establish whether they are limited to essential services.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
13.2.1	<p><i>Information transfer policies and procedures</i></p> <p>Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.</p>	We have inquired about data transfer policies and procedures.	No deviations noted.
13.2.2	<p><i>Agreements on information transfer</i></p> <p>Agreements address the secure transfer of business information between the organisation and external parties.</p>	<p>We have inquired about data transfer agreements.</p> <p>We have inquired into agreements with customers and other external parties, describing the requirements for safe exchange of data.</p>	No deviations noted.
13.2.3	<p><i>Electronic messaging</i></p> <p>Information involved in electronic messaging is appropriately protected.</p>	We have inquired about guidelines for electronic messaging of confidential information.	No deviations noted.

No.	Zentura A/S' control	REVI-IT's test	Test results
13.2.4	<p><i>Confidentiality or non-disclosure-agreements</i></p> <p>Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information, are identified, and documented on a regular basis.</p>	<p>We have inquired about the procedure for establishing non-disclosure-agreements.</p> <p>We have inspected a range of signed non-disclosure-agreements to establish whether the procedure has been followed when hiring of new staff and closing of agreements with consultants.</p>	No deviations noted.

A.15 Supplier relationships

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.	Zentura A/S' control	REVI-IT's test	Test results
15.2.1	<p><i>Monitoring and review of third-party services</i></p> <p>Organisations are regularly monitoring review and audit supplier service delivery.</p>	<p>We have inquired if the procedure for monitoring and review of services from subcontractors is according to the contract.</p> <p>We have inspected a range of status meeting minutes and operations reports, which are used to ensure that services rendered are according to the contract.</p> <p>Vi have inspected that review and evaluation of relevant audit reports about subcontractors, have been performed.</p>	No deviations noted.
15.2.2	<p><i>Manage changes to the third-party services</i></p> <p>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 reevaluation of risks involved.</p>	<p>We have inquired about management of changes with the subcontractor, and we have inspected the documentation for handling this.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
16.1.1	<p><i>Responsibilities and procedures</i></p> <p>Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.</p>	<p>We have inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities.</p> <p>Further, we have inspected the procedure for handling information security incidents.</p>	<p>We have observed that there have been no information security breaches during the audit period (01-11-2020 - 30-10-2021), which is why we have not been able to verify the effectiveness of the company's relevant procedure.</p> <p>No deviations noted.</p>
16.1.2	<p><i>Reporting information security events</i></p> <p>Information security events are being reported through appropriate management channels as quickly as possible.</p>	<p>We have inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines.</p>	<p>No deviations noted.</p>
16.1.3	<p><i>Reporting security weaknesses</i></p> <p>Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.</p>	<p>We have inquired about information security events during the period and we have inspected these.</p>	<p>No deviations noted.</p>
16.1.4	<p><i>Assessment of and decision on information security events</i></p> <p>Information security events are assessed, and it is decided if they are to be classified as information security incidents.</p>	<p>We have inquired into the procedure for assessment, response and evaluation of information security breaches.</p>	<p>No deviations noted.</p>
16.1.5	<p><i>Response to information security incidents</i></p> <p>Information security incidents are responded to in accordance with the documented procedures.</p>	<p>We have – by sample test - inspected that information security incidents have been responded to, in accordance with the documented procedures.</p>	<p>No deviations noted.</p>

No.	Zentura A/S' control	REVI-IT's test	Test results
16.1.6	<p><i>Learning from information security incidents</i></p> <p>Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.</p>	We have inquired about Problem-Management function which analyses information security incidents in order to reduce probability of recurrence.	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.	Zentura A/S' control	REVI-IT's test	Test results
17.1.1	<p><i>Planning information security continuity</i></p> <p>Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.</p>	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	<p><i>Implementing information security continuity</i></p> <p>Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.</p>	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.
17.1.3	<p><i>Verify review and evaluate information security continuity</i></p> <p>The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.</p>	<p>We have inquired about test of the contingency plan, and we have inspected documentation for tests performed.</p> <p>We have also inquired into reassessment of the contingency plan, and we have inspected documentation for reassessment.</p>	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.	Zentura A/S' control	REVI-IT's test	Test results
18.2.1	<p><i>Independent review of information security</i></p> <p>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.</p>	We have observed, that independent evaluation of information security has been established.	No deviations noted.
18.2.2	<p><i>Compliance with security policies and standards</i></p> <p>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.</p>	We have inquired into management's procedures for compliance with security policies and security standards.	No deviations noted.
18.2.3	<p><i>Technical compliance review</i></p> <p>Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.</p>	We have inquired into internal controls to ensure compliance with security policies and procedures, and we have inspected selected controls.	No deviations noted.