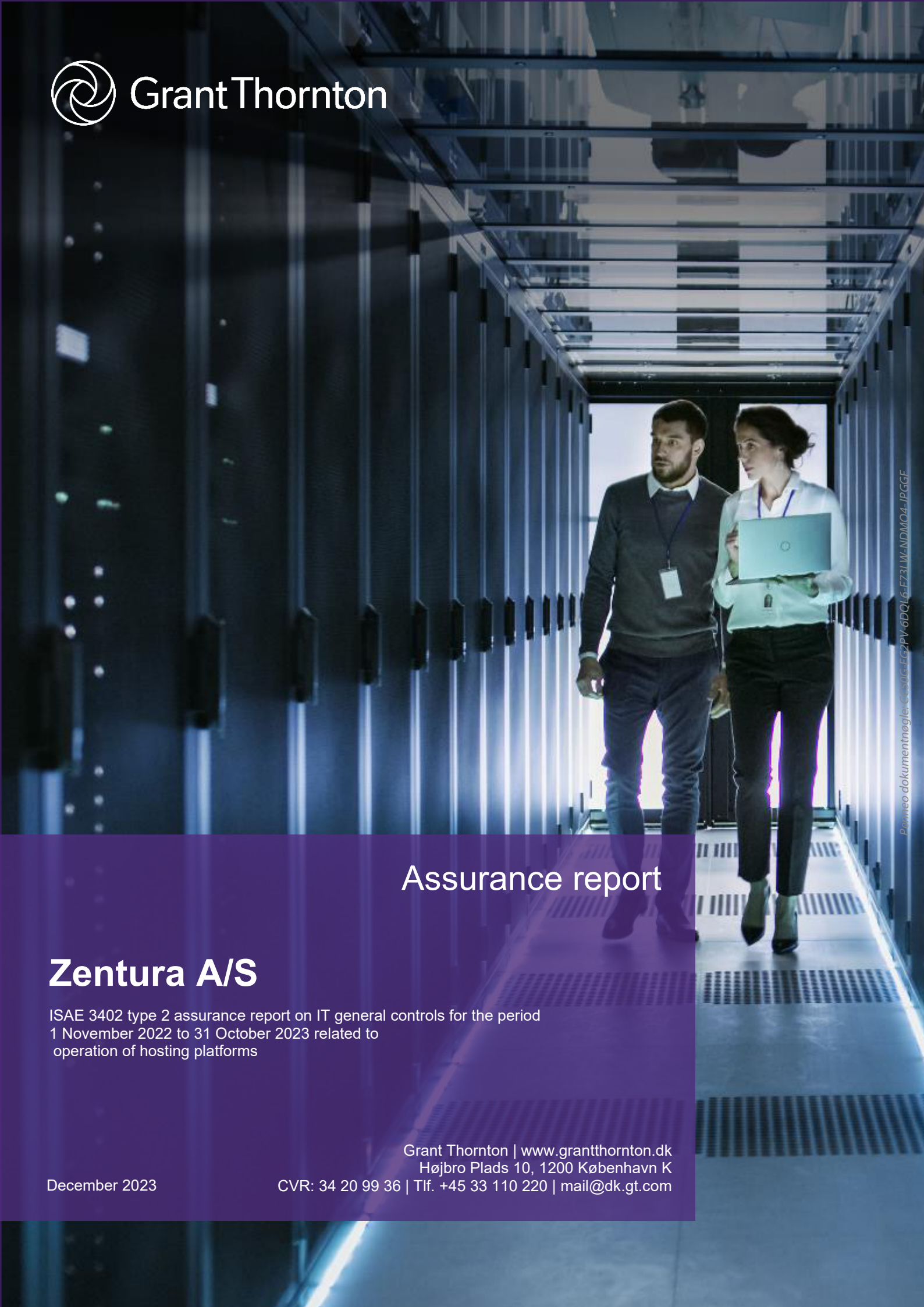

Assurance report

Zentura A/S

ISAE 3402 type 2 assurance report on IT general controls for the period 1 November 2022 to 31 October 2023 related to operation of hosting platforms

December 2023

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: Zentura A/S' statement

The accompanying description has been prepared for customers who have used Zentura A/S' hosting of platforms, 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 Microsoft, Interxion Danmark ApS, and Global Connect A/S. 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 Microsoft, Interxion Danmark ApS, and Global Connect A/S. Certain control objectives in the description can only be achieved, if the subsupplier's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subsuppliers.

Some of the control areas, stated in Zentura A/S' description in Section 3 of IT general controls, can only be achieved if the complementary controls with the customers are suitably designed and operationally effective with Zentura A/S' controls. This assurance report does not include the appropriateness of the design and operational effectivity of these complementary controls.

Zentura A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Zentura A/S' operation of hosting platforms processing of customer transactions throughout the period 1 November 2022 to 31 October 2023. 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, used to manage IT general 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 us alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

(ii) Contains relevant information about changes in the IT general controls, performed during the period 1 November 2022 to 31 October 2023

(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 operational effective during the period 1 November 2022 to 31 October 2023 if relevant controls with the subsupplier were operationally effective and the customers have performed the complementary controls, assumed in the design of Zentura A/S' controls during the entire period from 1 November 2022 to 31 October 2023. 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 2022 to 31 October 2023.

Taastrup, 18 December 2023
Zentura A/S

Christian Pedersen
CEO

Section 2: Independent service auditor's assurance report on the description of controls, their design and operating effectiveness

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

Scope

We have been engaged to report on a) Zentura A/S' description in Section 3 of its system for delivery of Zentura A/S' operation of hosting platforms throughout the period 1 November 2022 to 31 October 2023 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the description.

Zentura A/S is using subservice organisations Microsoft, Interxion Danmark ApS, and Global Connect A/S. 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 Microsoft, Interxion Danmark ApS, and Global Connect A/S. Certain control objectives in the description can only be achieved if the subsupplier's controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subsuppliers.

Some of the control objectives stated in Zentura A/S' description in Section 3 of IT general controls, can only be achieved if the complementary controls with the customers 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 in Section 3 and accompanying statement in Section 1 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.

Grant Thornton's independence and quality control

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

Grant Thornton 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.

Auditor's responsibility

Our responsibility is to express an opinion on Zentura A/S' description in Section 3, as well as on the design and operating effectiveness 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 in Section 3.

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 3, 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' statement in Section 1 and based on this, it is our opinion that:

(a) The description of the IT general controls, as they were designed and implemented throughout the period 1 November 2022 to 31 October 2023, 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 2022 to 31 October 2023 in all material respects, if controls with subsuppliers were operationally effective and if the customers have designed and implemented the complementary controls assumed in the design of Zentura A/S' controls during the period 1 November 2022 to 31 October 2023
(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 2022 to 31 October 2023.

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 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, 18 December 2023

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Description of Zentura A/S' services in connection with operating of hosting platforms, and related IT general controls

The following is a description of Zentura A/S' services which are included in the IT general 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.

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

IT General Controls at Zentura A/S

Introduction
In the following, a description of the IT General Controls related to Zentura A/S' services to customers, according to the above description in paragraph 1.1.

Use of subservice organizations

Zentura A/S uses several significant subservice organisations in connection with the supply of hosting platform.

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 partly specific work actions and partly processes for a number of work actions, which may also include further specific controls. 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 management

Registration, assessment, mitigation, and risk evaluation are an integrated 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

6.1.1 Roles and responsibilities for information security

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 etc. are involved and informed if relevant. The company's CEO and partner are responsible for the company's information security.

6.1.2 Internal organization

A limited number of people have access to internal servers in the Datacentres. In Azure Datacentres, PIM is used to control access.

6.1.4 Internal organization

We gather relevant information such as security updates and marked changes from newsletter subscriptions and commercial security sources.

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

6.2.1 Policy for mobile devices

We have no data-bearing media, except server room media, mobile phones and company enrolled Windows computers. On 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. All computers are enrolled with Microsoft Autopilot and managed through Intune. Bitlocker is forced on all Computers.

7. Human resource 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 repeatedly 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.

Employees who do not follow the rules can be sanctioned via their employment contract. Consultants via their contract and the signed NDA.

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 Liability for assets

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

All employees must follow the internal guidelines for using Zentura systems.

When an employee leaves the company all data and equipment must be returned.

9. Access control

Access is strictly given based on the role in the company. Critical access to core system is restricted to a limited team, and certain credentials are only accessible by management.

9.1. Business requirements for access control

Our customers' users are created, changed, and deleted 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. For 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.

2-factor authentication is mandatory for all employees and for all customers.

Users must only have access to the networks and network services that they are specifically authorized to use.

9.2 Managing user access

Business Cloud: User access is managed through AD Access Groups on a need to know/use basis.

Business Cloud 365: User access is managed through Microsoft PIM and Access Groups.

Zentura performs review of user access rights on a monthly basis.

9.3 User responsibility

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. Control of system and application access

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

11.1 Secure areas

Business Cloud
All our equipment is located in a separate rack at our data centre supplier. Only our technical staff has access here. Our backup equipment is located in its own rack at an alternative data centre location, at another data centre supplier. Our data centre vendors (Interxion and Global Connect) have ISAE 3402- II type auditor's statements, which are filed annually, and we obtain the same annually. In addition, we supervise our physical equipment when we regularly are at the location to perform necessary hardware related work. Our physical office is located in Taastrup.

Business Cloud 365
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. We do not have physical access to Azure datacentres.

11.2 Equipment
Zentura has implemented screensaver policies on all devices via group policy management.

12. Operations security

12.1 Operating procedures and responsibilities

12.1.2 Change Management
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 ITL 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 disk, CPU and traffic, and we can continuously, and without inconvenience to customers, expand our capacity.

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 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 e-mails (incoming and outgoing) are scanned for viruses by an external provider. We monitor our systems on a daily basis 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, enabling us to identify which people have been logged on.

12.4.1 Event logging
All systems are monitored using Zabbix. Events are logged automatically in Zabbix, and a mail are forwarded into the Service Desk and must be marked "Handled" before it is removed from the Service Desk.

12.4.2 Protection of log information
Events are registered in both Zabbix and immediately in the Service Desk at the same time. This makes it very difficult to change logs without being noticed and it would demand a detailed knowledge about our system setup, to avoid being discovered.

12.4.3 Administrator and operator log
Activities performed by the system administrator and system operator are logged in Remote Desktop Management and reviewed regularly.

12.4.4 Time synchronization
NTP time synchronization is used on all relevant systems.

12.5 Management of operating 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 3rd party programs such as Java, Adobe Reader, etc. 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 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 mails 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.

15. Supplier relationships

15.2. Management of supplier services
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

6.1 Management of information security breaches 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 fora, etc.

16.2 Follow-up on information security breaches
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

17.1.1 Information security continuity planning
A risk analysis has been established, which lists the possible scenarios that may affect the operation of our systems, and contingency plan 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.

17.1.2 Implementation of information security continuity
Should an emergency arise, Zentura has prepared a contingency plan. The contingency plan has been prepared in accordance with our IT security policy and our risk analysis, and it is maintained at least annually.

17.1.3 Verify, review and evaluate information security continuity
The plan is tested, and both the plan and procedures are anchored in our operational documentation and procedures. Our contingency planning takes into account that we can deliver our services on time at any time - almost no matter what happens.

18. Compliance

18.2 Review of information security
We are audited annually by an external auditor in order 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.

Information systems are regularly checked for compliance with company security policies and standards.

Changes during the period

There have been no significant changes in the audit period.

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
v) Request for access to the customer's server environment for the customer's third-party suppliers
vi) Customer's notification to the Data Inspectorate, for whom this may be relevant.

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

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

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.

Controls, which are specific to the individual customer solutions, or are performed by Zentura A/S' customers, are not included in this report.

Tests performed

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. Inquiries have included questions on how controls are being performed.
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. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general 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*	*Grant Thornton'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. We have inspected that an employee information security policy is approved and communicated to the employees.	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, that the information security policy has been reviewed, based on updated risk assessments, 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 organisation

No.	*Zentura A/S' control*	*Grant Thornton'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 inspected 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 organisations' assets.	We have inspected procedures regarding granting and maintenance of segregation of duties and functions.	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 that contact is maintained with special interest groups concerning the procedure security forums 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***	***Grant Thornton'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.	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.	***Zentura A/S' control***	***Grant Thornton'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 inspected the procedure for employment of new employees and the security measures needed in the process. We have, by sample test, 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 are stating their and the organisation's responsibilities for information security.	We have, by sample test, inspected an employee contract to determine whether the employee has signed.	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**	**Grant Thornton'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 organisation.	We have inspected the procedure for establishing requirements for employees and partners. We have inspected that management has required that employees observe the information security policy.	No deviations noted.
7.2.2	*Information security awareness education and training* Employees of the organisation are receiving appropriate education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inspected procedures securing adequate training and education.	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 to the employees.	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***	***Grant Thornton'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 and communicated to the employee or contractor and enforced.	We have, by sample test, inspected employees' 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.	*Zentura A/S' control*	*Grant Thornton'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 inspected guidelines for the use of assets.	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 inspected the procedure for securing the return of assets delivered, and we have, by sample test, inspected that the procedure is being followed.	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	Grant Thornton'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 inspected the access control policy 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 inspected how access to networks and network services are managed, and we have inspected the solution.	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	Grant Thornton'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 inspected the procedure for registration and de-registration of users. We have, by sample test, inspected documentation for registration and de-registration 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 inspected 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.	Zentura A/S' control	Grant Thornton'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 inspected procedures for granting of rights, use and limitation of privileged access rights. We have inspected 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 costumer 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 inspected the process of periodic review of users and we have, by sample test, inspected checks for review.	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 inspected procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected a terminated employee and we have inspected whether 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.	***Zentura A/S' control***	***Grant Thornton's test***	***Test results***
9.3.1	*Use of secret authentication information* Users are required to follow the organisations' 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.	***Zentura A/S' control***	***Grant Thornton's test***	***Test results***
9.4.2	*Secure log-on procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected the procedure for secure logon.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inspected that policies and procedures require quality passwords We have inspected that systems for administration of access codes are configured in accordance with the requirements.	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.	Zentura A/S' control	Grant Thornton'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 inspected policy for the use of encryption.	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	Grant Thornton'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 inspected the procedure for physical security of facilities and security perimeters. We have inspected 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 inspected the process for access control to secure areas.	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 inspected that physical security has been applied to protect offices, rooms, and facilities.	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***	***Grant Thornton's test***	***Test results***
11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	We have inspected the procedure for protection of unattended equipment.	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***	***Grant Thornton's test***	***Test results***
12.1.1	*Documented operating procedures* Operating procedures have been documented and made available to all users.	We have inspected that documentation for operating procedures is available to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure regarding changes of information handling equipment and -systems. We have, by sample test, inspected whether a selection of changes is approved, documented, and implemented in the production environment, according to the change management procedure.	No deviations noted.
12.1.3	*Capacity management* The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inspected the procedure for monitoring use of resources and adjustments of capacity, to meet future capacity requirements.	No deviations noted.

A.12.3 Backup Control objective: To protect against loss of data			
No.	***Zentura A/S' control***	***Grant Thornton'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 inspected configuration of backup and we have inspected samples of documentation for the setup. We have inspected that backup is monitored.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***Zentura A/S' control***	***Grant Thornton's test***	***Test results***
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inspected user activity logging. We have inspected that logs are reviewed on a regular basis.	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 inspected secure log information and we have inspected the solution. We have inspected logging configurations to establish whether login information is protected against manipulation and unauthorized access.	We have observed that internal IT have full access and can delete logs. We have observed that Zentura has accepted the associated risk. No further deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have inspected procedures regarding logging of activities performed by system administrators and operators.	No deviations noted.

No.	Zentura A/S' control	Grant Thornton's test	Test results
12.4.4	*Clock synchronization* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inspected the process 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.	**Zentura A/S' control**	**Grant Thornton'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 inspected software installation guidelines on operating systems and we have, by sample test, inspected that the guidelines are being followed.	No deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***Zentura A/S' control***	***Grant Thornton'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 inspected the policy regarding gathering and evaluation of technical vulnerabilities. We have inspected documentation for third party patch information on vulnerabilities.	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 inspected restriction of user executed software installations. We have inspected settings regarding restriction on software installation.	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	Grant Thornton's test	Test results
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	Vi have inspected that review and evaluation of relevant audit reports about subcontractors, have been performed.	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	Grant Thornton'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 inspected the responsibilities and procedures of information security incidents, and we have inspected documentation of the distribution of responsibilities. Further, 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 inspected guidelines for reporting information security incidents and weaknesses.	No deviations noted.

No.	Zentura A/S' control	Grant Thornton's test	Test results
16.1.3	*Reporting security weaknesses* 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.	We have inspected the proces for rapporting information security weaknesses.	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 inspected the procedure for assessment, response and evaluation of information security events.	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, by sample test, inspected that information security incidents have been responded to, according to the documented procedures.	No deviations noted.
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 inspected about problem management function which analyses information security incidents 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	Grant Thornton's test	Test results
17.1.1	*Planning information security continuity* 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.	We have inspected the preparation of a contingency ensuring 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* Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	We have inspected 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	*Verify review and evaluate information security continuity* 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.	We have inspected test of the contingency plan, and we have inspected documentation for tests performed. We have also inspected reassessment of the contingency plan, and we have inspected documentation for reassessment.	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*	*Grant Thornton'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 inspected management's procedures for compliance with security policies and security standards.	No deviations noted.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Christian Pedersen
Underskriver 1
Serial number: 9261d3a2-b6e6-42e9-9712-51865b427068
IP: 109.70.xxx.xxx
2023-12-20 09:14:34 UTC

Mit ID

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2023-12-20 09:17:15 UTC

Mit ID

Kristian Randløv Lydolph
Underskriver 3
Serial number: 7b9e0bc5-648f-4c07-87a8-debb5e403de6
IP: 62.243.xxx.xxx
2023-12-21 07:08:23 UTC

Mit ID

Penneo document key: CC50G-EG2PV-6DQL6-F73LW-NDMQ4-JPGGF