Assurance report

Zylinc A/S

ISAE 3402 type 1 assurance report on IT general controls related to the Zylinc Cloud solution as per April 30th, 2024.

June 2024

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: Zylinc A/S' statement

The accompanying description has been prepared for customers who have used Zylinc A/S' Zylinc Cloud solution, 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.

Zylinc A/S is using the subservice organisation Microsoft Corporation. This assurance report is prepared in accordance with the carve-out method and Zylinc A/S' description does not include control objectives and controls within Microsoft Corporation. Certain control objectives stated in the description can only be achieved, if the subservice organisation's controls as assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subservice organisations.

Zylinc A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Zylinc A/S' Zylinc Cloud solution, processing customer transactions as per April 30th, 2024.

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) 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 as per April 30th, 2024, if relevant controls with subservice organisations were operationally effective as per April 30th, 2024. 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

Copenhagen, June 20th, 2024
Zylinc A/S

Peter Stig Andersen
Chief Executive Officer

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

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

Scope

We have been engaged to report on a) Zylinc A/S' description in Section 3 of its system for delivery of Zylinc A/S' services as per April 30th, 2024, (the description) and on the design and operation of controls related to the control objectives stated in the description.

Zylinc A/S is using subservice organisation Microsoft Corporation. This assurance report is prepared in accordance with the carve-out method and Zylinc A/S' description does not include control objectives and controls within Microsoft Corporation. Certain control objectives in the description can only be achieved, if the subservice organisations' controls, assumed in the design of Zylinc A/S' controls, are suitably designed and operationally effective. The description does not include control activities performed by the subservice organisation.

Zylinc A/S' responsibility

Zylinc A/S is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Zylinc 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 Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on Zylinc A/S' description (Section 3) as well as on the design 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 (IASSB).

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.

An assurance engagement to report on the description and design 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 of controls.

The procedures selected depend on the service supplier's auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed. Our actions have included test of the implementation of such controls, that we regard as necessary to obtain a reasonable assurance, that the control objectives stated in the description were obtained.

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 and described in Section 1.

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

Zylinc 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.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in Zylinc A/S' section 1 and based on this it is our opinion, in all material respects:

(a) The description fairly presents the service-platform system as designed and implemented as per April 30th, 2024.

(b) The controls related to the control objectives stated in the description were suitably designed as per April 30th, 2024, to obtain reasonable assurance that the control objectives, stated in the description would be obtained if controls with the subservice organisations were operationally efficient.

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 Zylinc A/S' Zylinc Cloud solution 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, June 20th, 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Description of Zylinc A/S' services in connection with operation of Zylinc Cloud solution, and related IT general controls

Introduction to Zylinc A/S

Zylinc A/S is a Danish software company located in Copenhagen. Zylinc develops and markets solutions for Unified Communications with a focus on the customer service domain in our customers organisation. We market our solutions primarily through a partner channel, with a focus on the cloud-based Software-as-a-Service offering Zylinc Cloud.

Introduction to Zylinc's information security management system (ISMS)

The scope of Zylinc's Information Security Management System (the "ISMS") is the operational security of our Zylinc Cloud offering.

The structural basis for Zylinc's ISMS is the control requirements from ISO 27001:2022. An assessment to identify the relevant control requirements for Zylinc has been conducted and documented in a Statement-of-Applicability ("SoA"), setting out the organisational, technical, people, and physical controls found relevant by Zylinc for the proper operation of Zylinc Cloud for our customers.

The Statement-of-Applicability (SoA) will be reassessed yearly together with a yearly internal audit of the ISMS and the results will be part of the input to the yearly management review represented by Zylincs top-management. As an outcome from this meeting, changes to the ISMS structure and content are identified and implemented, ensuring proper risk mitigation and compliance with any new/changed requirements found relevant.

The current resulting structure of the ISMS and summaries of the information security policies and procedures laid down herein is described in the following.

Summary of the ISMS

An overall scoping factor for the SoA is the use of an external operational platform for Zylinc Cloud, i.e. Microsoft Azure. Furthermore, the ISMS is focused on the operational information security of Zylinc Cloud. Hence, Zylinc has identified 41 of 93 ISO27001 Annex A controls as appropriate for our information security, with the following policies, procedures, and controls as the result.

Organisational controls

Policy for information security
This is our top-level security policy in which our top management declares our commitment to measures and controls set out in our ISMS as well as the top-level governance and central roles established for the enforcement hereof.

Risk management
Our risk management procedure encapsulates two main activities: (1) Based on the assets included in our delivery of Zylinc Cloud, a thorough risk assessment is conducted for each asset. Each identified risk is evaluated and scored, and depending on its score a proper mitigation is decided and planned and (2) as the ISO27001 structure is used for the identification of the proper set of controls to safeguard Zylinc's operation of Zylinc Cloud, the lack of controls is perceived as a risk. Hence, a review of the Statement-of-Applicability of the controls of ISO27001 is an included part of Zylinc's risk management procedure.

Internal audit
Our internal audit procedure is the formal walk-through of our operational enforcement of the controls and activities of our ISMS. The internal audit is conducted shortly before our management review, and an internal audit report will summarize the results being the input to the management review.

Management review
The management review is the yearly top-level assessment of the information security state in Zylinc. Among the materials used in the management review, the results of the risk management procedure and the internal audit are some of the most important. The management meeting minutes documents the actions decided, and the CISO is accountable for its execution.

Information security assessment
A joined collaboration between CISO and CTO secures the necessary procedures for maintaining a high level of information security. Information security considerations are integrated into the product development process as new projects are started. This ensures ongoing awareness from employees.

Asset management
Essential management and control of assets are structured and the necessary on- and offboarding procedures take care of the implementation of keeping the information up to date and allowing the necessary overview to consider potential risks.

On- and offboarding of employees
Our procedure for on- and offboarding employees includes checklists ensuring that employees with a potential security impact on the operation of Zylinc Cloud is screened and granted the right need-to access to Zylinc Cloud assets, as well as having such access closed when leaving their position with Zylinc. Further, our employment contracts include information security requirements for our employees, both during and after their employment with Zylinc.

Access management and -control
The least-privilege principle is used for assigning new access to employees handled through structured on- and offboarding procedures, including department head approval, and existing accesses are reviewed once a year. Multi-factor authentication is mandatory for critical systems.

Handling security incidents
A structured procedure for handling security incidents is in place and includes post-mortem reporting to ensure that learning is documented and adopted. The same procedure is used for major incidents that are not necessarily categorised as a security incident.

Information security roles and responsibilities
Sets out the roles, forums and named employees having the main responsibilities in the ISMS.

Management responsibilities
Lists the ISMS policies and procedures anchoring our management's responsibilities and documentation for the information security requirements set forth in our employee contracts.

Monitoring, review and change management of supplier services
Procedures are put in place for handling cloud service changes and assessing SLAs, access management and data protection.

Information security during disruption (Disaster/Recovery)
Incident procedures and severity outlines are in place, as well as a disaster recovery plan.

Independent review of information security
Our documentation is in the form of our ISAE3402 external auditor report.

Compliance with policies, rules and standards for information security
This control includes our "annual wheel" of high-level ISMS repeatable activities as well as a documented list of policies and procedures in the ISMS ensuring compliance.

People controls

Screening of employees
Our procedure for screening employees sets out the screening activities when joining and during employment with Zylinc to be carried out for employees with a potential security impact on the operation of Zylinc Cloud.

Information security training
Mandatory security awareness training is mandatory for new joiners and yearly for all existing employees. The awareness training is updated (and potentially rerun) based on current global security landscape.

Disciplinary process
Our documentation of the explicit disciplinary sanctions for employees' breach of information security policies and procedures requirements as set out in employees' employment contracts.

Responsibilities after termination or change of employment
Our documentation of the explicit statement to employees when terminating or changing a position.

Technological controls

Information access restrictions
The least-privilege principle is used for assigning new access to employees handled through structured on- and offboarding procedures, including department head approval, and existing accesses are reviewed once a year. Multi-factor authentication is mandatory for critical systems.

Access to source code
Strict access control is applied to code repositories and other locations that potentially contain source code. Access is reviewed yearly and updated as part of on- and offboarding procedures.

Backup
Systems and services with vital data for the operation are backed up on a regular basis. Backups are placed in geographically diverse locations, or in the case of Azure using their industry-standard backup. Regular reviews after infrastructure changes are carried out. Backups happen in connection with patches.

Logging
Critical systems generate comprehensive logs that record user activities, and the log is protected against unauthorized access, tampering and accidental loss.

Software installs
A flexible approach to software installs is in place, where employees are permitted to install software that they deem necessary for their work. A recommended list of software is available. This approach is measured against the assessed risk and will be reviewed yearly.

Security of network services
Network devices are configured according to industry best practices and secured against unauthorized access. Ingress traffic is encrypted using standard TLS 1.2 or similar. Network changes follow internal procedures for change management.

Infrastructure capacity management
Systems are in place to monitor capacity and utilization of critical systems related to Zylinc Cloud. Metrics are monitored daily and selected automated alarms are put in place including assigned employees to on-call schedules.

Software development
Zylinc Cloud is developed using PIs (program increments) which consists of five (5) two (2) week sprints. The development flow goes through planning, design and prototyping, development and coding, continuous integration and testing, deployment, monitoring and feedback, and review and continuous improvement. Deployment is handled in batches of tenants assessed by their risk profile and availability needs.

Changing production environments
A formal procedure is ensuring proper planning, approval, pre-change testing, backup and documentation, implementation, post-change review and reporting.

Selecting test data
Data used for testing are in most cases restricted to be either auto generated or manually inserted as part of development and quality assurance flows. Customer data is rarely used, and if so, a procedure for assessing risks is in place.

Secure authentication
MFA are required for privileged user accounts and VPN required for user access to internal network resources.

Protection against malware
Anti-malware software is mandatory for all devices.

Use of privileged utility programs
Privileged utility programs are documented, and regular reviews are carried out.

Separation of development, test, and production environments
Environments are segregated and require different privileges for access.

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 Zylinc A/S' subservice organisations.

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

Tests

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

Method	General description
Inquiries	Interview with appropriate employees at Zylinc 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 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 Zylinc A/S.

A.5 Organisational controls

Control objective: To ensure continuing suitability, adequacy, effectiveness of management direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.1	*Policies for information security* Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant employees and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant stakeholders. We have inspected that the information security policy is updated.	No deviations noted.
5.2	*Information security roles and responsibilities* Information security roles and responsibilities should be defined and allocated according to the organisation's needs.	We have inspected documentation that responsibility for information security is clearly defined and allocated.	No deviations noted.
5.4	*Management responsibilities* Management should require all employees to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.	We have inspected that the management has required that employees must comply with information security policies and procedures.	No deviations noted.

A.5 Organisational controls

Control objective: To establish a management framework that ensures the identification and mitigation of information security risks related to legal, regulatory, supervisory authorities, threats and project management.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.8	*Information security in project management* Information security should be integrated in project management.	We have inspected that a project management procedure covering information security requirements has been designed.	We have been informed that no projects, as of now, have followed the new project management procedure. No deviations noted.

A.5 Organisational controls

Control objective: To identify organisational assets and define appropriate protection responsibilities.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.9	*Inventory of information and other associated assets* An inventory of information and other associated assets, including owners, should be developed and maintained.	We have inspected that an inventory of assets, including owners, is developed and maintained.	No deviations noted.
5.11	*Return of assets* Employees and other interested parties as appropriate should return all the organisation's assets in their possession upon change or termination of their employment, contract or agreement.	We have inspected that a procedure for return of assets has been designed. We have, by sample test, inspected that employees upon termination of employment have returned assets to the organisation.	No deviations noted.

A.5 Organisational controls

Control objective: To ensure authorized access and to prevent unauthorized access to information and other associated assets.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.15	*Access control* Rules to control physical and logical access to information and other associated assets should be established and implemented based on business and information security requirements.	We have inspected that an access management policy and procedure has been designed and updated.	No deviations noted.
5.16	*Identity management* The full life cycle of identities should be managed.	We have inspected that identities are assigned unique user IDs that enable the traceability of actions performed. We have inquired about the assignment and removal of user access rights.	We have been informed that no employee has been on- or offboarded since the implementation of a new identity and access management procedure as of 1st May 2024. No deviations noted.
5.17	*Authentication information* Allocation and management of authentication information should be controlled by a management process, including advising employees on the appropriate handling of authentication information.	We have inspected that a password management procedure has been designed. We have inspected that the password configuration settings are in accordance with the defined procedure.	No deviations noted.
5.18	*Access rights* Access rights to information and other associated assets should be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy on and rules for access control.	We have inspected the access control procedure. We have inquired if access rights have been reviewed on a regular basis and at least annually.	We have been informed that no employee has been on- or offboarded since the implementation of a new identity and access management procedure as of 1st May 2024. We have inspected that a review of access rights has been planned but is not yet completed. No further deviations noted.

A.5 Organisational controls

Control objective: To maintain an agreed level of information security in supplier relationships and service delivery in line with supplier agreements.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.22	*Monitoring, review and change management of supplier services* The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	We have inspected that monitoring activities, covering outsourced supplier services, have been performed for all significant suppliers.	No deviations noted.
5.23	*Information security for use of cloud services* Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	We have inspected that information security measures covering the use of cloud services has been defined and implemented.	No deviations noted.

A.5 Organisational controls

Control objective: To ensure a quick, effective, consistent and orderly approach to the management of information security incidents, including communication on security events and weaknesses.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.24	*Information security incident management planning and preparation* The organisation should plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	We have inspected that an incident management procedure has been designed. We have inspected that roles and responsibilities related to the incident management procedure has been defined.	No deviations noted.

No.	Zylinc A/S' control	Grant Thornton's test	Test results
5.25	*Assessment and decision on information security events* The organisation should assess information security events and decide if they are to be categorised as information security incidents.	We have inspected how information security events are assessed and categorised.	No deviations noted.
5.26	*Response to information security incidents* Information security incidents should be responded to in accordance with the documented procedures.	We have inspected the procedure for responding information security incidents. We have inquired into whether information security incidents have occurred.	We have been informed that no information security incidents have occurred. No deviations noted.
5.27	*Learning from information security incidents* Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	We have inspected the procedure for learning from information security incidents. We have inquired into whether information security incidents have occurred.	We have been informed that no information security incidents have occurred. No deviations noted.

A.5 Organisational controls

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

No.	Zylinc A/S' control	Grant Thornton's test	Test results
5.29	*Information security during disruption* The organisation should plan how to maintain information security at an appropriate level, during disruption.	We have inspected that a business contingency plan has been designed. We have inspected that the business contingency plan is made available to relevant employees. We have inquired if the business contingency plan has been tested.	We have inspected that a test of the business contingency plan has been planned but not yet completed. No further deviations noted.

A.5 Organisational controls

Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
5.35	*Independent review of information security* The organisation's approach to managing information security and its implementation including people, processes and technologies, should be reviewed independently at planned intervals, or when significant changes occur.	We have inspected that an independent review of the organisation's information security has been performed covering the implementation and operation in accordance with policies and procedures.	No deviations noted.
5.36	*Compliance with policies, rules and standards for information security* Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	We have inspected that the organisation has defined a list of controls for compliance with policies and procedures.	We have inspected that the internal controls for compliance with policies and procedures have been planned but not yet completed. No further deviations noted.

A.6 People controls

Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
6.1	*Screening* Background verification checks of all candidates before hiring, should be carried out prior to joining the organisation and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional with the business requirements, the classification of the information to be accessed and the perceived risks.	We have inspected that a procedure for screening of new employees has been designed. We have, by sample test, inspected that background verification checks have been performed for new employees in accordance with the procedure.	No deviations noted.
6.2	*Terms and conditions of employment* The employment contractual agreements should state the employee's and the organisation's responsibilities for information security.	We have, by sample test, inspected that signed employment agreements state the employee's and the organisation's responsibilities for information security.	No deviations noted.

A.6 People controls

Control objective: To ensure employees and relevant interested parties are aware of and fulfil their information security responsibilities as well as understand the consequences of information security policy violations.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
6.3	*Information security awareness, education and training* The organisation's employees and relevant interested parties should receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant to their job function.	We have inspected that an information security awareness programme has been established. We have inspected that the organisation's employees have completed the information security awareness training.	No deviations noted.
6.4	*Disciplinary process* A disciplinary process should be formalized and communicated to take actions against employees and other relevant interested parties who have committed an information security policy violation.	We have inspected that a disciplinary process has been established and communicated to relevant employees. We have, by sample test, inspected that signed employment agreements state the consequences of information security policy violations.	No deviations noted.

A.6 People controls

Control objective: To protect the organisation's interests as part of the process of changing or terminating employment

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
6.5	*Responsibilities after termination or change of employment* Information security responsibilities and duties that remain valid after termination or change of employment should be defined, enforced and communicated to relevant employees and other interested parties.	We have inspected that information security responsibilities and duties that remain valid after termination or change of employment have been defined. We have, by sample test, inspected that terminated employees have been informed that information security responsibilities and duties is still valid after termination of employment.	No deviations noted.

A.8 Technological controls

Control objective: To ensure that the allocation and use of privileged access rights have been restricted and controlled to reduce the risk of unauthorized access, changes to systems and inaccurate authentication.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
8.2	*Privileged access rights* The allocation and use of privileged access rights should be restricted and managed.	We have inspected that a procedure for administration of privileged access rights has been designed. We have inspected that privileged access rights are restricted to a work-related need.	No deviations noted.
8.3	*Information access restriction* Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	We have inspected that an access management policy and procedure have been designed and updated. We have inspected that access rights are restricted to a work-related need.	No deviations noted.
8.4	*Access to source code* Read and write access to source code, development tools and software libraries should be appropriately managed.	We have inspected that access to source code has been limited to employees with a work-related need.	No deviations noted.
8.5	*Secure authentication* Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	We have inspected that a password management procedure has been designed. We have inspected that the password configuration settings are set in accordance with the defined procedure. We have inspected that multi-factor authentication are installed and enabled.	No deviations noted.

A.8 Technological controls

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

No.	Zylinc A/S' control	Grant Thornton's test	Test results
8.6	*Capacity management* The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	We have inspected that a procedure for monitoring use of resources and adjustments of capacity has been designed. We have inspected that information processing resources are being monitored. We have inspected that detective controls are implemented to identify problems.	No deviations noted.
8.7	*Protection against malware* Protection against malware should be implemented and supported by appropriate user awareness.	We have inspected that a procedure for protection against malware has been designed. We have, by sample test, inspected that anti-malware has been implemented on mobile devices.	No deviations noted.

A.8 Technological controls

Control objective: To ensure the continuous operation of information processing facilities including the recovery from loss of data or systems.

No.	Zylinc A/S' control	Grant Thornton's test	Test results
8.13	*Information backup* Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	We have inspected that a procedure for backup of data has been designed. We have, by sample test, inspected that backup copies are made continuously in accordance with the procedure. We have inspected that regular tests are performed of backup data to verify that the data can be restored from backup files.	No deviations noted.

A.8 Technological controls

Control objective: To record events, generate evidence, ensure the integrity of log information, prevent against unauthorized access, detect anomalous behaviour and identify information security events and incidents.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
8.15	*Logging* Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	We have inspected that a procedure for log management has been designed. We have inspected that logs are configured in accordance with the procedure. We have inspected that logs collected are protected against manipulation or deletion.	No deviations noted.

A.8 Technological controls

Control objective: To ensure the integrity of operational systems and application controls as well as prevent exploitation of technical vulnerabilities.

No.	*Zylinc A/S' control*	*Grant Thornton's test*	*Test results*
8.19	*Installation of software on operational systems* Procedures and measures should be implemented to securely manage software installation on operational systems.	We have inspected that a procedure for installation of software on operational systems has been designed. We have inspected that installation of software on operational systems has been protected.	No deviations noted.

A.8 Technological controls

Control objective: To ensure the protection of information in networks and its supporting information processing facilities.

No.	Zylinc A/S' control	Grant Thornton's test	Test results
8.21	*Security of network services* Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	We have inspected that a network security policy has been designed. We have inspected that firewalls are installed and updated on the network.	No deviations noted.
8.22	*Segregation of networks* Groups of information services, users and information systems should be segregated in the organisation's networks.	We have inspected that network segmentation is implemented which divides the network into multiple zones.	No deviations noted.

A.8 Technological controls

Control objective: To ensure information security is designed and implemented within the secure development life cycle of software and systems.

No.	Zylinc A/S' control	Grant Thornton's test	Test results
8.25	*Secure development life cycle* Rules for the secure development of software and systems should be established and applied.	We have inspected that a procedure for secure development life cycle has been designed.	No deviations noted.
8.26	*Application security requirements* Information security requirements should be identified, specified and approved when developing or acquiring applications.	We have, by sample testing, inspected that security requirements are identified, specified and approved when developing or acquiring applications.	No deviations noted.

No.	Zylinc A/S' control	Grant Thornton's test	Test results
8.27	*Secure system architecture and engineering principles* Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities.	We have inspected secure system architecture and engineering principles.	No deviations noted.

A.8 Technological controls

Control objective: To ensure that changes to applications, database systems, and associated infrastructure are properly authorized, documented, tested, approved, and implemented in the production environment.

No.	Zylinc A/S' control	Grant Thornton's test	Test results
8.31	*Separation of development, test and production environments* Development, testing and production environments should be separated and secured.	We have inspected that development, testing and production environments are separated.	No deviations noted.
8.32	*Change management* Changes to information processing facilities and information systems should be subject to change management procedures.	We have inspected that a change management procedure has been designed. We have, by sample test, inspected that key stakeholders have approved changes prior to release into production. We have, by sample test, inspected that changes are tested based on established criteria prior to release into production.	No deviations noted.
8.33	*Test information* Test information should be appropriately selected, protected and managed.	We have inspected that a procedure for test information has been designed. We have inquired about the availability of test information.	We have been informed that no copying of operational information to test environments have occurred within the last 3 months. No deviations noted.

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."

Peter Stig Andersen
Underskriver 1
Serial number: 8e4e347a-f32b-4cba-81ac-c94f6fb1488d
IP: 78.153.xxx.xxx
2024-06-20 11:59:43 UTC

Andreas Moos
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 2
Serial number: 8ba4bf1c-2aac-4cbe-9a4b-48056ec67035
IP: 62.243.xxx.xxx
2024-06-20 12:01:28 UTC

Kristian Randløv Lydolph
Grant Thornton, Godkendt Revisionspartnerselskab CVR: 34209936
Underskriver 3
Serial number: 84758c07-82ce-4650-a48d-5224b246b5c4
IP: 62.243.xxx.xxx
2024-06-21 10:41:43 UTC