INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT FOR THE PERIOD FROM 1 MAY 2024 TO 30 JUNE 2025 ON THE DESCRIPTION OF ZYLINC CLOUD AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

ZYLINC A/S

BDO

INDHOLD

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ASSURANCE REPORT FOR THE PERIOD FROM 1 MAY 2024 TO 30 JUNE 2025 ON THE DESCRIPTION OF ZYLINC CLOUD AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATIONG EFFECTIVENESS

To: Management of Zylinc A/S
Zylinc's customers and their auditors

Scope

We have been engaged to report on the description in section 3 prepared by Zylinc A/S (the service provider) for the period from 1 May 2024 to 30 June 2025 of its ZYLINC CLOUD service and related controls, and on the design and operating effectiveness of controls related to the control objectives stated in the description.

The service provider's responsibilities

The service provider is responsible for preparing the statement in section 2 and the accompanying description, including the completeness, accuracy and the manner in which the statement and description is presented.

Furthermore, the service provider is responsible for providing the services included in the description, as well as for stating the control objectives and designing and implementing effectively operating controls to achieve the control objectives stated.

The information in section 5 – Supplementary information from Zylinc A/S is not part of Zylinc A/S' description of services. The information in section 5 has not been subject to the procedures performed by BDO as part of the assessment of the description in section 3.

Auditor's independence and quality assurance

We have complied with the requirements for independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence and due diligence, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret Revisionspartnerselskab applies International Standard on Quality Management 1 (ISQM 1) which requires that we design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legislation and other regulation.

Auditor's responsibilities

Our responsibility is, on the basis of our procedures, to express an opinion on the service provider's description and on the design and operational efficiency of controls related to the control objectives set out in this description.

We have performed our work in accordance with International Standard on Assurance Engagements 3402 on controls at a service provider. This standard requires that we plan and perform our procedures in order to obtain reasonable assurance of whether the description is correct in all material respects and whether the controls in all material respects are suitably designed and have operated effectively.

An assurance engagement to issue an opinion on the description and design, and operational

efficiency of controls at a service provider includes performing procedures to obtain evidence of the information of the service provider's description as well as of the controls' design and operational efficiency. The selected procedures depend on the assessment by the service auditor, including the assessment of the risks that the description is not accurate and that the controls are not suitably designed or do not operate effectively. Our actions have included tests of the operational efficiency of such controls, which we consider necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. An assurance engagement of this type also includes an assessment of the overall presentation of the description, the appropriateness of the control objectives stated therein, and the appropriateness of the criteria specified and described by the service provider in section 2.

We believe that the evidence obtained is sufficient and appropriate to provide a basis for our opinion.

Restrictions in controls at a service organisation

The service providers' description is prepared to meet the common needs of a wide range of the company's customers and their auditors and, therefore, it may not include every aspect of the application of the ZYLINC CLOUD which each individual customer may consider important in their own particular environment. Moreover, due to their nature, controls at a service provider may not prevent or detect all errors or omissions at the processing or reporting of transactions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters accounted for in this report. The criteria we used in forming our opinion are those described in the service provider's statement in section 2. It is our opinion that:

a. The description of ZYLINC CLOUD and the relating controls, as designed and implemented throughout the period from 1 May 2024 to 30 June 2025 is in all material respects are presented fairly, and

b. The controls related to the control objectives stated in the description, in all material respects, were suitably designed and implemented throughout the period from 1 May 2024 to 30 June 2025, and

c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 May 2024 to 30 June 2025.

Description of tests of controls

The specific controls which were tested, and results of those tests, are listed in section 4.

Intended users and purpose

This report is intended only for customers, who have used the service provider's ZYLINC CLOUD services, and their auditors who have a sufficient understanding to consider it along with other information, including information about the customer's own controls, when obtaining an understanding of the customers' information systems relevant to the financial reporting.

Copenhagen, 22 August 2025

BDO Statsautoriseret Revisionspartnerselskab

Nicolai T. Visti
Partner, State Authorised Public Accountant

Mikkel Jon Larssen
Partner, Head of Risk Assurance, CISA, CRISC

2. ZYLINC'S STATEMENT

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.

The accompanying description has been prepared for Zylinc's customers and their auditors, who have a sufficient understanding to consider ZYLINC CLOUD along with other information, including information about controls used by the customers themselves, when obtaining an understanding of customers' information systems relevant to the financial reporting.

Zylinc uses sub-service providers. The subservice providers' relevant control objectives and related technical and organizational measures and other controls are not included in the accompanying description.

Zylinc confirms that the accompanying description in section 3 fairly presents ZYLINC CLOUD and the related controls for the period from 1 May 2024 to 30 June 2025. The criteria used in making this statement were that the accompanying description:

1. Accounts for the ZYLINC CLOUD, and how the related controls were designed and implemented, including accounts for:

    - The services which are provided,
    - The processes in both IT systems and manual systems which are used to provide ZYLINC CLOUD,
    - Relevant control objectives and controls designed to achieve these objectives.
    - Controls which we have assumed would be implemented by the user companies with reference to the design of the system, and which, if necessary to achieve the control objectives stated in the description, are identified in the description along with the specific control objectives we cannot achieve ourselves.
    - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls which have been relevant to the processing and reporting of customer transactions.

2. Includes relevant details of changes to the controls relating to the delivery of ZYLINC CLOUD during the period from 1 May 2024 to 30 June 2025.

3. Does not omit or distort information relevant to the scope of ZYLINC CLOUD and the related controls considering that this description has been prepared to meet the general needs of a wide range of customers and their auditors and, therefore, it cannot include every aspect of ZYLINC CLOUD which the individual customer may consider of importance to their special environment.

Zylinc confirms that the controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively for the period from 1 May 2024 to 30 June 2025. The criteria for making this statement were that:

1. The risks threatening the achievement of the control objectives stated in the description were identified.

2. The identified controls would, if performed as described, provide reasonable assurance that those risks did not prevent the achievement of the control objectives stated.

Copenhagen, 22 August 2025

Zylinc A/S

Peter Stig Andersen
CEO

3. ZYLINC'S DESCRIPTION OF ZYLINC CLOUD

GENERAL DESCRIPTION OF ZYLINC CLOUD

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.

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

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) is being reassessed yearly together with a yearly internal audit of the ISMS and the results are part of the input to the yearly management review represented by Zylinc's 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 are described in the following.

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 53 of 93 ISO27001 Annex A controls as appropriate for our information security, with the following policies, procedures, and controls as the result.

Risk assessment

On a yearly basis, Zylinc performs a risk assessment, which includes IT installations and the use thereof. The risk assessment is based on the current threat scenario and is part of the documentation for the annual IT audit. Based on the recommendations of the audit, the risk assessment may form the basis for new projects, which are to increase the information security of Zylinc's IT platforms.

This report includes solely controls and control objectives for processes and controls that are managed by Zylinc and, thus, it does not include controls or control objectives, that are managed by subservice organisations.

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR IMPLEMENTATION OF CONTROLS

Zylinc's information security is defined on the basis of the objective of providing an online application software service infrastructure solutions, including stability and security.

The determination of criteria and scope of the implementation of controls at Zylinc is based on the ISO 27002:2022 framework for information security management. The following control areas of ISO 27002 were assessed:

- A.5 Organisational controls
- A.6 People controls
- A.7 Physical controls
- A.8 Technological controls

Implemented control environment
The implemented controls are based on the services provided by Zylinc to customers, and they include control areas and control activities within the delivery of an online application software service. All of the above areas are separately summarized in the following paragraphs, and the described control objectives and controls for these areas in the paragraph on control objectives, controls, tests and result of tests are an integral part of the description.

A.5: Organisational controls

A.5.1 Policies for information security
Zylinc's top-level security policy confirms management's commitment to the ISMS and defines governance and central roles. It is backed by procedures for risk management, including asset-based assessments and SoA reviews, internal audits to verify operational enforcement of controls, and annual management reviews where key findings and actions are documented and followed up by the CISO.

A.5.2 Information security roles and responsibilities
Zylinc has established a clear and approved structure for ISMS roles and responsibilities. The document defines key individuals and forums involved, including the ZLT (Zylinc Leadership Team) and ISB (Information Security Board), with formal confirmation of responsibilities. The CISO ensures role alignment, while HR must notify the CISO of any personnel changes impacting ISMS governance.

A.5.3 Segregation of duties
Zylinc applies segregation of duties where feasible to reduce the risk of error or misuse of systems. In areas where full separation is not practical due to company size, compensating controls such as peer reviews, approvals, and monitoring are implemented to ensure accountability.

A.5.4 Management responsibility
Zylinc's management ensures that all employees follow the company's information security policy, including topic-specific policies and procedures, by setting clear expectations and promoting a culture of accountability.

A.5.8 Information security in project management
Zylinc integrates information security assessments into projects involving changes to data handling in Zylinc Cloud. Assessments are conducted at project start or scope changes to identify and mitigate risks. Responsibilities are shared across Product Managers, the CTO, and Tech Architect, ensuring risks are addressed through documented actions and oversight.

A.5.9 Inventory of information and other associated assets
Zylinc maintains an up-to-date asset inventory covering employee-assigned laptops, phones, and monitors. The IT Manager ensures asset records are created during onboarding, updated as needed, verified at offboarding, and reviewed annually to track ownership and plan upgrades.

A.5.11 Return of assets
Zylinc's onboarding and offboarding procedure ensures that employees are screened, granted appropriate access, and trained in information security. Upon termination, all physical and digital assets are collected or

disabled. Responsibilities are clearly assigned across HR, IT, Finance, and People Managers to enforce compliance and protect company assets and data.

A.5.15 Access control
Zylinc enforces access controls based on least privilege and need-to-know principles for all systems and facilities related to Zylinc Cloud. Access is granted with proper authorization, reviewed at least annually, and revoked immediately when no longer needed. MFA is required for critical systems, and all exceptions and incidents must be formally documented and handled.

A.5.16 Identity management
Zylinc manages system and physical access through a controlled, role-based identity management process. Access is granted via documented requests and approvals, maintained by IT, and overseen by the CTO. Reviews are conducted at least annually, with immediate revocation upon role changes or termination. MFA is applied where relevant, and all incidents are formally reported and investigated.

A.5.17 Authentication information
Zylinc enforces strong password practices to protect access to systems and data. Passwords must be complex, securely distributed, and regularly updated. The IT department manages policy enforcement, while all users are trained annually on password security. Initial credentials are provided securely, and MFA is applied where required.

A.5.18 Access rights
Zylinc manages access rights through its onboarding and offboarding procedure, ensuring access is granted, adjusted, or revoked based on role changes and employment status to maintain proper control over system and data access.

A.5.19 Information security in supplier relationships
Zylinc defines information security requirements for all sub-service providers and limits their system access strictly to what is needed for their assigned tasks, reducing exposure to unnecessary risks.

A.5.20 Addressing information security within supplier agreements
Zylinc includes information security requirements in supplier agreements on a case-by-case basis, considering the nature of the service and associated risks. The approach is pragmatic and adapted to the company's size and operational context.

A.5.22 Monitoring, review and change management of supplier services
Zylinc has focused on onboarding and offboarding suppliers but plans to strengthen periodic reviews going forward to ensure supplier services continue to meet information security expectations.

A.5.23 Information security for use of cloud services
Zylinc applies a structured but practical approach to adopting and reviewing cloud services. New and existing services are evaluated for business fit, security features, compliance, and encryption standards, with oversight by the CTO and operational responsibility held by the IT Manager.

A.5.24 Information security incident management planning and preparation
Zylinc has a structured procedure for detecting, prioritizing, and responding to security incidents to minimize impact and maintain service continuity. Incidents are classified by urgency and impact, with P0 triggering potential disaster recovery. DevOps leads initial response, the CTO oversees resolution, and all actions are documented in internal systems.

A.5.29 Information security during disruption
Zylinc maintains a disaster recovery plan to handle major incidents affecting Zylinc Cloud, such as ransomware, infrastructure failures, or region-wide outages. Disasters are defined as events with the potential to disrupt customer operations for over 24 hours. Key personnel are designated for response and communication, with recovery objectives guiding the structured execution of mitigation efforts.

A.5.35 Independent review of information security & A.5.36 Compliance with policies, rules and standards for information security
Zylinc conducts independent reviews of its information security through the established internal audit and management review procedures defined in section 5.1, ensuring regular oversight and continuous improvement of the ISMS.

A.6: People controls

A.6.1 Screening
Zylinc screens personnel in security-trusted positions to reduce risk and ensure suitability. Background checks are performed during hiring and annually thereafter, covering criminal records, qualifications, and references, with documentation maintained by HR in accordance with legal and risk-based considerations.

A.6.2 Terms and conditions of employment
Zylinc includes information security responsibilities in employment contracts, clearly defining both employee and organizational obligations to ensure awareness and accountability from the start of employment.

A.6.3 Information security awareness, education and training
Zylinc ensures all personnel receive information security training during onboarding and through annual refreshers. Training covers organizational policies, threat awareness, and role-specific responsibilities. The program is maintained by the CTO, coordinated by HR, and regularly updated by IT to reflect evolving risks.

A.6.5 Responsibilities after termination or change of employment
Our documentation of the explicit statement to employees when terminating or changing a position.

A.6.8 Information security event reporting
Zylinc handles security event reporting through the incident management procedure defined in section 5.24, ensuring timely detection, documentation, and escalation of security-related events.

A.7: Physical controls

A.7.1 Physical security perimeters
Zylinc has implemented procedures and controls to ensure that IT equipment is properly protected against unauthorised physical access and environmental incidents.

A.7.2 Physical entry
Zylinc's premises have access control in the form of a required personal code and a system key to ensure that only authorised staff has access. Only Zylinc's employees will receive a key and a code. If suppliers, consultants or other external parties need access, this is only possible together with authorised staff.

A.8: Technological controls

A.8.2 Privileged access rights & A.8.3 Information access restriction
Zylinc restricts and manages access to systems and assets according to defined access control policies. Privileged access is tightly controlled and granted only as needed, ensuring alignment with job roles and minimizing the risk of misuse.

A.8.4 Access to source code
Zylinc ensures that read and write access to source code, development tools, and software libraries is controlled and granted only where necessary, protecting the integrity of development environments and preventing unauthorized changes.

A.8.5 Secure authentication
Zylinc enforces secure authentication in line with its access control policies under A.8.2, ensuring appropriate technologies and procedures are applied to protect access to systems and data.

A.8.6 Capacity management
Zylinc continuously monitors and reviews infrastructure capacity to meet current and projected demands for Zylinc Cloud. DevOps and IT maintain performance metrics and planning, with biannual reviews and ad-hoc assessments. Plans are aligned with business growth and communicated to stakeholders, led by the CTO.

A.8.7 Protection against malware
Zylinc protects against malware using Intune-managed policies to ensure Microsoft Defender is active and up to date. This technical control is supported by user awareness through general security training.

A.8.8 Management of technical vulnerabilities
Zylinc manages technical vulnerabilities primarily through bi-annual penetration tests. Findings are logged and assessed in Azure DevOps, with critical issues tracked through dedicated follow-up actions by Team DevOps. This ensures vulnerabilities are identified, evaluated, and addressed systematically to maintain a strong security posture.

A.8.13 Information backup
Zylinc performs regular, structured backups of critical data for Zylinc Cloud, using geographically diverse storage including Azure. Backup integrity is ensured through scheduled restore tests and monitored logs. Failed backups are promptly investigated, and the backup policy is reviewed annually to stay aligned with operational and compliance needs.

A.8.15 Logging
Zylinc maintains logs of relevant system activities, exceptions, and faults as a baseline control. Based on risk assessment, a pragmatic approach is applied with limited review procedures currently in place. Plans are in place to expand log management efforts over time.

A.8.18 Use of privileged utility programs
Zylinc restricts access to utility programs that can bypass system or application controls, ensuring only authorized personnel are permitted to use such tools to maintain system integrity and prevent misuse.

A.8.19 Installation of software on operational systems
Zylinc permits employees to install work-relevant software at their discretion, while encouraging use of a pre-approved list maintained by IT. Licensed installations must be reported, and the organization reserves the right to revoke any installation that poses a security risk. This balanced policy supports productivity while maintaining oversight.

A.8.20 Networks security
Zylinc's network is structured to prevent direct internet access to application servers unless explicitly defined. Network protection is enforced using established firewall technologies to safeguard internal infrastructure.

A.8.21 Security of network services & A.8.22 Segregation of networks
Zylinc identifies and implements essential security measures for network services based on risk assessment. While current monitoring and review are limited, a pragmatic approach is applied, with plans to expand oversight and service-level evaluations over time. Data in transit is encrypted using at least TLS 1.2.

A.8.25 Secure development life cycle
Zylinc follows a flexible but structured secure development process based on DevOps principles, incorporating CI/CD, code reviews, automated testing, and monitored releases. Security is embedded throughout the lifecycle, with responsibilities shared across developers, QA, and DevOps under CTO oversight.

A.8.26 Application Security Requirements
Zylinc ensures that information security requirements are identified, specified, and approved when developing or acquiring applications. This is integrated into the development lifecycle to align with product and risk considerations.

A.8.27 Secure System Architecture and Engineering Principles
Zylinc applies secure design principles across all systems, guided by best practices, risk assessments, and internal priorities. Systems are configured securely, monitored, and subject to annual security assessments to maintain a resilient and compliant environment.

A.8.30 Outsourced development
Zylinc supervises outsourced development by applying the same onboarding, offboarding, and access control principles used for internal hires. This ensures consistent oversight and alignment with security requirements throughout the engagement.

A.8.31 Separation of development, test and production environments
Zylinc maintains separation between development, testing, and production environments to reduce the risk of unauthorized changes and ensure system stability and data integrity.

A.8.32 Change management
Zylinc enforces a controlled change management process for production systems, with changes planned, approved, tested, and documented. Risk level determines the required approvals and testing, and all high-risk changes include rollback procedures and post-change reviews to ensure service continuity and system integrity.

A.8.33 Test information
Zylinc ensures test data is securely managed and does not include customer or personal data. Synthetic or anonymized data is used to support effective testing while protecting sensitive information. Any exceptions follow a defined process led by DevOps and developers.

CHANGES IN THE PERIOD FROM 1 MAY 2024 to 30 JUNE 2025

Zylinc has not made any significant changes to ZYLINC CLOUD and the associated technical and organizational security measures and other controls in the period from 1 May 2024 to 30 June 2025.

COMPLEMENTARY CONTROLS AT THE SERVICE PROVIDER

The customer is obligated to implement the following technical and organisational security measures and other controls to achieve the control objectives and thereby comply with relevant legislation:

- The customer is responsible for ensuring that the administrators' use of ZYLINC CLOUD is in accordance with relevant legislation.
- The customer controls the user privileges on ZYLINC CLOUD, including to whom administrator access is allocated and which rights are granted to the individual administrators.

4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

Objective and scope

BDO has performed the work in accordance with International Standard on Assurance Engagements (ISAE) 3402 relating to controls at a service provider.

BDO has performed procedures to obtain evidence of the information of Zylinc's description of ZYLINC CLOUD and of the design, implementation and operating effectiveness of these relating controls. The selected procedures depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed operating effectively.

BDO's test of the design of controls and the implementation hereof have included the control objectives and related control activities selected by Zylinc A/S, and which are described in the following control form.

In the control form, BDO has described the tests performed and considered necessary to obtain reasonable assurance about whether the stated control objectives were achieved and whether the related controls were suitably designed and operated effectively throughout the period from 1 May 2024 to 30 June 2025.

Performed test procedures

Tests of the design of controls and the implementation and operating effectiveness hereof were performed by inquiry, inspection, observation and re-performance.

Type	Description
Inquiry	Inquiries with relevant personnel at Zylinc A/S have been made for all significant control activities. The inquiries were made to obtain knowledge and additional information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures and controls.
Inspection	Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, including whether the controls are designed so that they may be expected to become effective, if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals. Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.
Re-performance	Controls have been re-performed to obtain additional evidence that the controls operate as assumed.

For the services provided by Microsoft Azure within hosting, we have from an independent auditor received a SOC 1 report for the period from 1 April 2024 to 31 March 2025 on technical and organisational security measures.

For the services provided by Zendesk within support services, we have from an independent auditor received a SOC 2 report for the period from 1 October 2024 to 31 March 2025 on technical and organisational security measures.

For the services provided by Elastic.IO within processing of statistics, we have from an independent auditor received a SOC 2 report for the period from 1. November 2023 to 31 October 2024 on technical and organisational security measures.

For the services provided by Speechmatics within transcription speech to text services, we have from an independent auditor received a SOC 2 report for the period from 1 September 2024 to 30 November 2024 on technical and organisational security measures.

These sub-service providers' relevant control objectives and related controls are not included in Zylinc A/S' description of services and relevant controls related to operation of Zylinc A/S' Outsourcing Services. Accordingly, we have solely assessed the report and tested the controls at Zylinc A/S that monitor the operating effectiveness of the sub-service provider's controls.

Result of test

The result of the tests performed indicates whether the described test has given rise to note exceptions.

An exception exists when:

- Controls have yet to be designed or implemented to fulfil a control objective.
- Controls related to a control objective are not suitably designed, implemented or operating effectively.

Risk assessment			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Risk assessment To ensure that the service provider performs an annual risk assessment in relation to the foundation of the technical and organisational security measures.	▶ A risk assessment of ZYLINC CLOUD is performed currently, and at least once a year, based on potential risks to data availability, confidentiality and integrity. ▶ The vulnerability of systems and processes are assessed based on identified threats. ▶ Risks are minimised based on the assessment of their probability, consequences and derived implementation costs. ▶ Risk assessments are updated currently, but at least once a year.	We have made inquiries with relevant personnel. We have inspected the service provider's risk management procedure and observed that is has been updated during the declaration period, and that the risk register is based on risks to confidentiality, integrity and availability. We have inspected the service provider's risk register and observed that actions plans have been made for identified risks. We have inspected the service provider's risk register and observed that identified risks are assessed with a probability and consequence score.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Policies for information security To ensure current suitability, adequacy, effectiveness of Management's direction and support for information security in accordance with business, legal, statutory, regulatory and contractual requirements, according to ISO/IEC 27002 A.5.1.	▶ Information security policy and topic-specific policies should be defined, approved by management, published, communicated to relevant interested parties, and reviewed at planned intervals and if significant changes occur.	We have made inquiries with relevant personnel. We have inspected the service provider's information security policy and have observed that the policy and topic specific policies have been defined, approved by the senior management team, reviewed during the declaration period and communicated to relevant parties.	No exceptions noted.
Information security roles and responsibilities To establish a defined, approved and understood structure for implementation, operation and management of information security within the organisation, according to ISO/IEC 27002 A.5.2.	▶ Information security roles and responsibilities should be defined and allocated according to the organisation's needs.	We have made inquiries with relevant personnel. We have inspected that responsibility for information security is clearly defined and allocated.	No exceptions noted.
Segregation of duties To reduce the risk of fraud, errors and evasion of information security measures, according to I ISO/IEC 27002 A.5.3.	▶ The service provider's duties and areas of responsibility are segregated to the extent it is possible considering the size of the company, to reduce the possibility of unauthorised or unintentional use, modification or misuse of data.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for segregation of duties within IT and information security within the organisations infrastructure and observed that areas of duties and responsibilities have been segregated. We have inspected the service provider's topic specific policies and procedures and observed that the documents have been reviewed and approved by different personnel.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Management responsibilities To ensure that Management understands its role in information security and initiates procedures aiming to ensure all personnel is aware of and fulfil their information security responsibilities, according to ISO/IEC 27002 A.5.4.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's procedure for roles and responsibilities and observed that formal guidelines have been defined. We have inspected that the employees' responsibilities have been communicated. We have by random sample inspected documentation that the service provider's employees have acknowledged their responsibilities.	No exceptions noted.
Information security in project management To ensure information security risks related to projects and deliverables are effectively addressed in project management throughout the project life cycle, according to ISO/IEC 27002 A.5.8.	▶ Information security should be integrated in project management.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for information security within projects and have observed that a risk assessment for potential threats against the infrastructure shall be carried out. We have inspected by random samples that appropriate risk assessments for projects during the declaration period have been carried out and observed that information security was integrated.	No exceptions noted.
Inventory of information and other associated assets To identify the organisation's information and other associated assets in order to maintain information security and assign appropriate ownership, according to ISO/IEC 27002 A.5.9.	▶ An inventory of information and other associated assets, including owners, should be developed and maintained.	We have made inquiries with relevant personnel. We have inspected that an inventory of assets, including owners, is developed and maintained.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Return of assets To protect the organization's assets as part of the process of changing or terminating employment, contract or agreement, according to ISO/IEC 27002 A.5.11.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's off-boarding procedure and observed that assets must be returned when employment is terminated. We have inspected by random samples that assets have been returned to the service provider upon termination of the employment.	No exceptions noted.
Access control To ensure authorised access and to prevent unauthorised access to information and other associated assets, according to ISO/IEC 27002 A.5.15.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's policy for access control and observed rules to control physical and logical access to information has been established and implemented. We have inspected the service provider's technical password configuration and observed that is it in line with the service provider's password policy.	No exceptions noted.
Identity management To allow for the unique identification of individuals and systems accessing the organisation's information and other associated assets and to enable appropriate assignment of access rights, according to ISO/IEC 27002 A.5.16.	▶ The service provider has established a procedure for registering and deregistering users in connection with the assignment of access rights.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for access management and observed that access is only granted based on a work-related need. Furthermore, we have observed that access is removed when employment is terminated.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		We have inspected by random samples that employees only have access to work-related resources and that terminated employees access rights have been revoked.	
Authentication information To ensure proper entity authentication and prevent failures of authentication processes, according to ISO/IEC 27002 A.5.17.	▶ Allocation and management of authentication information should be controlled by a management process, including advising employees on the appropriate handling of authentication information. The service provider manages the allocation of secret authentication information through a formal administration process.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for authentication information and observed that the service provider is using a password manager for safeguarding passwords and that passwords must be changed at first logon. We have inspected the service provider's configuration for password change at the first logon and observed, that it has been configured correctly. We have inspected the service provider's technical implementation for their password manager and observed that employees are allocated credentials resources based on their job role and work-related need.	No exceptions noted.
Access rights To ensure that access to information and other associated assets is defined and authorised in accordance with the business requirements, according to ISO/IEC 27002 A.5.18.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's procedure for access control and observed that access to resources granted is based on a work related. We have inspected by random samples that employees only have access to work-related resources and that terminated employees have	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		been removed from the service provider's systems. We have inspected documentation for periodic review of access to the service provider's resources and observed that a periodic review has been conducted during the declaration period.	
Information security in supplier relationships To maintain an agreed-upon level of information security in supplier relationships, according to ISO/IEC 27002 A.5.19.	▶ The service provider has established information security requirements to subservice providers used. ▶ The service provider has restricted the subservice provider's access to the service provider's systems in relation to the subservice provider's work-related needs.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for security in supplier relationships and observed that a risk assessment and evaluation must be conducted prior to implementation of a new supplier. We have inspected the service provider's documentation for risk assessment and evaluation for implementing new suppliers. We have inspected the service provider's periodic review of access to Zylinc Cloud and observed that all suppliers have been reviewed. By inquiry the service provider has informed that they have concluded that all suppliers access to Zylinc Cloud are sufficient restricted.	No exceptions noted.
Addressing information security within supplier agreements To maintain an agreed-upon level of information security and provision of services in accordance with the supplier agreements, according to ISO/IEC 27002 A.5.20.	▶ Information security requirements are agreed upon with relevant subservice providers.	We have made inquiries with relevant personnel. We have inspected the service provider's agreements with their suppliers and have observed that information security requirements are included in the agreements.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Monitoring, review and change management of supplier services To maintain an agreed-upon level of information security and provision of services in accordance with supplier agreements, according to ISO/IEC 27002 A.5.22.	▶ The organisation should regularly monitor, review, evaluate and manage changes in supplier information security practices and service delivery.	We have made inquiries with relevant personnel. We have observed that the service provider has conducted supervision of all relevant suppliers during the declaration period. We have inspected Microsoft's SOC 1 report from 1 April 2024 to 31 March 2025. We have inspected ZenDesk's SOC 2 report from 30 October 2024 to 31 March 2025. We have inspected Elastic.IO's SOC 2 report from 1 November 2023 to 31 October 2024. We have inspected Speechmatics' SOC 2 report from 1 September 2024 to 30 November 2024.	No exceptions noted.
Information security for use of cloud services To specify and manage information security in connection with the use of cloud services, according to ISO/IEC 27002 A.5.23.	▶ Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organisation's information security requirements.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for cloud services and observed that prior to establishing or exiting from a cloud service an evaluation must be performed. We have inspected the service provider's risk assessment and evaluation for a new cloud service and observed that it has been performed prior to implementation. By inquiry we have been informed that no cloud services have exited from the service provider during the declaration period.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Information security incident management planning and preparation To ensure prompt, effective, consistent and orderly response to information security incidents, including communication on information security events, according to ISO/IEC 27002 A.5.24.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's procedure for incident management and have observed that formal guidelines have been defined for roles and responsibilities, response, incident management and communication.	No exceptions noted.
Assessment and decision on information security events To ensure effective categorization and prioritization of information security events, according to ISO/IEC 27002 A.5.25.	▶ The organisation should assess information security events and decide if they are to be categorized as information security incidents.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for incident management and have observed that formal guidelines have been defined to assess and categorize information security incidents. We have by random samples inspected the service provider's incident reports from incidents that occurred during the declaration period and observed that the service provider's procedure for incident management has been followed.	No exceptions noted.
Response to information security incidents To ensure efficient and effective response to information security incidents, according to ISO/IEC 27002 A.5.26.	▶ Information security incidents should be responded to in accordance with the documented procedures.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for incident management and have observed that formal guidelines have been defined for incident response. We have by random samples inspected the service provider's incident reports from incidents	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		that occurred during the declaration period and observed that the service provider's procedure for incident management has been followed and a response for incident has been performed within reasonable time.	
Learning from information security incidents To reduce the likelihood or consequences of future incidents, according to ISO/IEC 27002 A.5.27.	▶ Knowledge gained from information security incidents should be used to strengthen and improve the information security controls.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for incident management and have observed that formal guidelines for evaluation and learning from incidents have been defined. By inquiry we have been informed that the service provider conducts a timeline and conclusion of an incident in their incident reports and evaluated when deemed needed. We have by random samples inspected the service provider's incident reports from incidents that occurred during the declaration period and observed that the service provider's procedure for incident management has been followed, and knowledge gained from information security incidents to strengthen and improve the information security.	No exceptions noted.
Information security during disruption To protect information and other associated assets during disruption, according to ISO/IEC 27002 A.5.29.	▶ The organisation should plan how to maintain information security at an appropriate level, during disruption.	We have made inquiries with relevant personnel. We have inspected that a business contingency plan has been designed, and recovery time objectives have been defined.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		We have inspected that a disaster recovery test has been performed during the declaration period. We have by random samples inspected the service provider's incident reports from incidents that occurred within the declaration period and observed that incidents have been resolved within a reasonable time.	
Independent review of information security To ensure the continuing suitability, adequacy and effectiveness of the organization's approach to managing information security, according to ISO/IEC 27002 A.5.35.	▶ 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 made inquiries with relevant personnel. By inquiry we have been informed that the service provider once annually gets their information security and its implementation, including people, processes and technologies, independently reviewed. We have inspected the service provider's agreement with an independent auditor and observed that the service provider have obligated them self for an annual independent review once annually.	No exceptions noted.
Compliance with policies, rules and standards for information security To ensure that information security is implemented and operated in accordance with the organization's information security policy, topic-specific policies, rules and standards, according to ISO/IEC 27002 A.5.36.	▶ Compliance with the organisation's information security policy, topic-specific policies, rules and standards should be regularly reviewed.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for internal audit and observed that includes the entire information security management system and must be conducted once annually.	No exceptions noted.

A.5 Organisational controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		We have inspected the service provider's annual cycle and observed that routine tasks have been performed during the declaration period. We have inspected documentation that an internal audit has been conducted during the declaration period.	
Documented operating procedures To ensure correct and secure operation of information processing facilities, according to ISO/IEC 27002 A.5.37	▶ Operating procedures have been prepared and made available for relevant employees.	We have made inquiries with relevant personnel. We have inspected the service provider's infrastructure and observed that all operating procedures have been made available for all relevant employees.	No exceptions noted.

A.6 People controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Screening To ensure that all employees are qualified for the roles, for which they are considered, and that they remain qualified during their employment, according to ISO/IEC 27002 A.6.1.	▶ Background verification checks of relevant 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 made inquiries with relevant personnel. We have inspected that a procedure for screening of new employees has been designed. We have, by random samples inspected that background verification checks have been performed for new employees in accordance with the procedure during the declaration period.	No exceptions noted.
Terms and conditions of employment To ensure personnel understand their information security responsibilities for the roles for which they are considered, according to ISO/IEC 27002 A.6.2.	▶ The employment contractual agreements should state the employee's and the organisation's responsibilities for information security.	We have made inquiries with relevant personnel. We have, by randoms samples, inspected that signed employment agreements state the employee's and the organisation's responsibilities for information security.	No exceptions noted.
Information security awareness, education and training To ensure that employees and relevant stakeholders are aware of and observe their information security responsibilities, according to ISO/IEC 27002 A.6.3.	▶ 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 made inquiries with relevant personnel. We have inspected that an information security awareness program has been established. We have inspected that the service provider's employees have completed the annually information security awareness training. We have by random samples inspected that new employees have received awareness training as part of their onboarding.	No exceptions noted.

A.6 People controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Responsibilities after termination or change of employment To protect the organization's interests as part of the process of changing or terminating employment or contracts. according to ISO/IEC 27002 A.6.5.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's procedure for offboarding and observed that leaving employees must be informed of their confidentiality obligations after termination of employment. We have by random samples inspected that leavers have been informed of their confidentiality obligations after termination of employment.	No exceptions noted.
Information security event reporting To support timely, consistent and efficient reporting of information security incidents which can be identified by employees, according to ISO/IEC 27002 A.6.8.	▶ The service provider reports information security incidents to relevant parties.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for incident management and observed that formal guidelines for communication have been established. By inquiry we have been informed that no incident within the declaration period have been deemed critical enough that external communication have been needed. We have by random samples inspected the service provider's incident reports from incidents occurred during the declaration period and observed that internal communication has been followed in accordance with the service provider's procedure.	No exceptions noted.

A.7 Physical controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Physical entry To ensure that only authorised physical access to the organisation's information and other associated assets occurs, according to ISO/IEC 27002 A.7.2	▶ Physical entry controls have been established to prevent the likelihood of unauthorised access to the service provider's offices and facilities, including to ensure that only authorised employees have access. ▶ Review of the physical access to the data processor's offices and facilities is performed currently and least once a year.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for physical entry and observed that entry must be protected with an electronic lock. We have inspected the service provider's office location and observed that access controls are implemented. We have inspected the service provider's documentation for periodic review of the physical entry to the service provider's offices and observed that it has been conducted during the declaration period.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Privileged access rights To ensure that only authorised users, software components and services are provided with privileged access rights, according to ISO/IEC 27002 A.8.2.	▶ The allocation and use of privileged access rights should be restricted and managed.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for privileged access and observed that access is granted on a least privileged principle. We have inspected the service provider's documentation for granted privileged access and observed, that all granted access is based on a work-related need. We have inspected the service provider's documentation for periodic review for privileged access and observed, that is has been conducted during the declaration period.	No exceptions noted.
Information access restriction To ensure only authorised access and to prevent unauthorised access to information and other associated assets, according to ISO/IEC 27002 A.8.3.	▶ Access to information and other associated assets should be restricted in accordance with the established topic-specific policy on access control.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for access control and observed that access is granted on a least privileged principle. We have inspected the service provider's infrastructure and observed that employees solely have access to resources where they have a work related need to access.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Access to source code To prevent unauthorised functionality, avoid unintentional or malicious changes and to maintain the confidentiality of valuable intellectual property, according to ISO/IEC 27002 A.8.4.	▶ Read and write access to source code, development tools and software libraries should be appropriately managed.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for access control to source code and observed that access to repositories solely is granted based on a work-related need. We have inspected the configuration of user rights in the service provider's development tool and observed that appropriate user rights have been configured. We have by random samples inspected that access to source code has been limited to employees with a work-related need.	No exceptions noted.
Secure authentication To ensure that a user or an entity is securely authenticated when access to systems, applications and services is granted, according to ISO/IEC 27002 A.8.5.	▶ Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for access control and observed multi factor authentication must be used when logging into critical IT-systems. We have inspected the service provider's multi factor authentication configuration and observed that all employees are included in the configuration.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Capacity management To ensure the required capacity of information processing facilities, human resources, offices and other facilities, according to ISO/IEC 27002 A.8.6.	▶ The use of resources should be monitored and adjusted in line with current and expected capacity requirements.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for monitoring use of resources and adjustments of capacity and observed that controls must be implemented to identify potential problems. We have inspected the monitoring tool and observed that resources and capacity use on the Zylinc Cloud platform are monitored. We have observed that the service provider receives notifications regarding potential resources and or resource issues.	No exceptions noted.
Protection against malware To ensure that information and other associated assets are protected against malware, according to ISO/IEC 27002 A.8.7.	▶ Protection against malware should be implemented and supported by appropriate user awareness.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for protection against malware and have observed that anti-virus and malware software must be installed on all workstations. We have inspected the anti-virus configuration and observed that all workstations are included. We have inspected the service provider's documentation for awareness training and observed that malware protection has been included in the training.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Management of technical vulnerabilities To prevent exploitation of technical vulnerabilities, according to ISO/IEC 27002 A.8.8.	▶ The service provider obtains information about technical vulnerabilities. ▶ The service provider has considered identified vulnerabilities.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for penetration testing and observed that at least once annually a penetration test must be conducted. We have observed that the service provider has performed a penetration test during the declaration period. We have by random samples inspected that identified vulnerabilities has been mitigated.	No exceptions noted.
Information backup To enable recovery from loss of data or systems, according to ISO/IEC 27002 A.8.13.	▶ 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 made inquiries with relevant personnel. We have inspected the service provider's backup procedure and observed that backup must be conducted regularly on critical systems and a restore test must performed as least once annually. We have inspected the service provider's critical systems and observed that backup is taken regularly and a restore test has been conducted during the declaration period.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Logging To record incidents, generate evidence, ensure the integrity of log information, prevent against unauthorised access, identify information security events which may lead to information security incidents and support investigations, according to ISO/IEC 27002 A.8.15.	▶ Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for logging and observed that access, user actions and abnormal user behaviour are logged, stored and protected. We have inspected the service provider's logs for access, user action and abnormal behaviour and observed, that they are logged, stored and protected within the service provider's infrastructure.	No exceptions noted.
Use of privileged utility programs To ensure that the use of utility programs does not harm system and application measures for information security, according to ISO/IEC 27002 A.8.18.	▶ Only authorised employees can access programs, which can bypass system and application controls.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for software instalment and observed that all employees are allowed to install software on their workstations.	We have concluded that all employees are able to install privileged utility programs on their workstations. No further exceptions noted.
Installation of software on operational systems To ensure the integrity of operational systems and prevent exploitation of technical vulnerabilities, according to ISO/IEC 27002 A.8.19.	▶ Procedures and measures should be implemented to securely manage software installation on operational systems.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for software instalments and observed that all employees are allowed to install software on their workstations.	We have concluded that software instalments on workstations are not managed. No further exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Network security To protect information in networks and supporting information processing facilities from compromising via the network, according to ISO/IEC 27002 A.8.20.	▶ The network topology is structured so that servers running applications only allow access directly from the internet on ports necessary to provide the SaaS offering. ▶ The service provider uses known network technologies and mechanisms (Firewall/Intrusion Detection System/Intrusion Prevention System) to protect the service provider's internal network.	We have made inquiries with relevant personnel. We have inspected the service provider's network topology and observed that the network is protected in a way that traffic is not able to directly communicate with the internet. We have inspected the service provider's network technology and observed that the network is protected with recognized technologies and mechanisms.	No exceptions noted.
Security of network services To ensure security in the use of network services, according to ISO/IEC 27002 A.8.21.	▶ Security mechanisms, service levels and service requirements of network services should be identified, implemented and monitored.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for network security and observed that the network must be protected with firewall mechanisms where firewall rules must be reviewed at least once annually. We have inspected that firewalls are installed on the network and that rules have been reviewed and validated during the declaration period.	No exceptions noted.
Segregation of networks To divide the network with security limitations and to control traffic between them based on business needs, according to ISO/IEC 27002 A.8.22.	▶ Groups of information services, users and information systems should be segregated in the organisation's networks.	We have made inquiries with relevant personnel. We have inspected that network segmentation is implemented.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Secure development life cycle To ensure information security is designed and implemented within the secure development life cycle of software and systems, according to ISO/IEC 27002 A.8.25.	▶ Rules for the secure development of software and systems should be established and applied.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for secure development and observed that rules have formally been defined for the development life cycle. We have by random samples inspected that development projects during the declaration period have followed the service provider's secure development procedure.	No exceptions noted.
Application security requirements To ensure all information security requirements are identified and addressed when developing or acquiring applications, according to ISO/IEC 27002 A.8.26.	▶ Information security requirements should be identified, specified and approved when developing or acquiring applications.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for secure development and observed that the service provider has defined requirements for development. We have by random samples inspected that development projects during the declaration period have followed the service provider's secure development procedure.	No exceptions noted.
Secure system architecture and engineering principles To ensure information systems are securely designed, implemented and operated within the development life cycle, according to ISO/IEC 27002 A.8.27.	▶ Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities	We have made inquiries with relevant personnel. We have inspected the service provider's architectural drawing for their infrastructure and observed it has been designed based on best	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		practise principles for engineering secure systems. We have inspected the service provider's infrastructure and observed that it has been configured in accordance with the architectural drawing.	
Outsourced development To ensure that the information security measures required by the organisation are implemented in outsourced system development, according to ISO/IEC 27002 A.8.30.	▶ The service provider supervises and monitors system development activities, which have been outsourced.	We have made inquiries with relevant personnel. We have by inquiry been informed that the service provider does not use external consultants for developing why the controls implementation and operational efficiency could not be tested.	We have established that the service provider has not used external consultants for developing during the declaration period. Therefore, we have not been able to test the control for implementation and effectiveness. No exceptions noted.
Separation of development, test and production environments To protect the production environment and data from compromise as a consequence of development and test activities, according to ISO/IEC 27002 A.8.31.	▶ Development, testing and production environments should be separated and secured.	We have made inquiries with relevant personnel. We have inspected that development, testing and production environments are separated.	No exceptions noted.
Change management To maintain information security when executing changes, according to ISO/IEC 27002 A.8.32.	▶ Changes to information processing facilities and information systems should be subject to change management procedures.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for change management and observed that a test must be conducted prior to the release into the production environment.	No exceptions noted.

A.8 Technological controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
		We have, by random samples inspected that changes are tested in accordance with the service provider's change management procedure and prior to deployment.	
Test information To ensure relevance of testing and protection of operational information used for testing, according to ISO/IEC 27002 A.8.33.	▶ Test information should be appropriately selected, protected and managed.	We have made inquiries with relevant personnel. We have inspected the service provider's procedure for test information and observed that no client data are allowed to be used in the test environments. We have inspected the service provider's test environments and have observed that no client data are used.	No exceptions noted.

5. SUPPLEMENTARY INFORMATION FROM ZYLINC A/S

The supplementary information below has not been the subject of the audit carried out by BDO.

Based on BDO's ascertained exceptions in the ISAE 3402 declaration, Zylinc A/S has the following supplementary information:

Control activity	Result of test	Comment of the company
8.18 Use of privileged utility programs ▶ Only authorised employees can access programs, which can bypass system and application controls.	We have concluded that all employees are able to install privileged utility programs on their workstations.	Zylinc acknowledges this finding. While Zylinc recognizes the importance of maintaining a secure and efficient computing environment, it also acknowledges the need for flexibility given our current size and risk assessment. As such, employees are permitted to install software that they deem necessary for their work, provided it does not violate any legal or licensing agreements. Employees are encouraged to exercise good judgment and discretion in selecting and installing software, prioritizing tools and applications that enhance productivity and operational efficiency without compromising security. This is aided by general security awareness training for everyone.
8.19 Installation of software on operational systems ▶ Procedures and measures should be implemented to securely manage software installation on operational systems.	We have concluded that software instalments on workstations are not managed.	Zylinc acknowledges this finding with the same comment as above.

BDO STATSAUTORISERET REVISIONSPARTMERSEÆSLAN

VESTRE RINGGADE 28
8000 AARHUS C

www.bdo.dk

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Peter Stig Andersen
CEO
På vegne af: ZYLINC A/S
Serienummer: 8e4e347a-f32b-4cba-81ac-c94f6fb1488d
IP: 78.153.xxx.xxx
2025-08-26 15:13:50 UTC

Mit ID

Nicolai Tobias Visti Pedersen
BDO 2025 Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner, State Authorised Public Accountant
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 62.66.xxx.xxx
2025-08-26 15:47:57 UTC

Mit ID

Mikkel Jon Larssen
BDO Holding VII, statsautoriseret revisionsaktieselskab CVR: 20222670
Partner, Head of Risk Assurance, CISA, CRISC
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff
IP: 77.243.xxx.xxx
2025-08-27 07:30:02 UTC

Mit ID