ONLINECITY.IO

ONLINECITY.GROUP ApS

ISAE 3402 Assurance Report 2026

gatewayapi

BDO

CONTENT

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ASSURANCE REPORT FOR THE PERIOD 1 MAY 2025 TO 30 APRIL 2026 ON THE DESCRIPTION OF GATEWAYAPI AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

To: The Management of ONLINECITY Group ApS
ONLINECITY GROUP ApS' customers

Scope
We have been engaged to report on the description in section 3 prepared by ONLINECITY Group ApS (the service provider) for the period from 1 May 2025 to 30 April 2026 of its GatewayAPI and related controls, and on the design and operating effectiveness of controls related to the control objectives stated in the description.

ONLINECITY Group ApS uses subservice providers in connection with their role as service providers. This assurance report has been prepared using the partial method and therefore does not include control objectives and controls at these subservice providers.

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.

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 GatewayAPI 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 organisation 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 GatewayAPI and the relating controls, as designed and implemented throughout the period from 1 May 2025 to 30 April 2026 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 2025 to 30 April 2026, 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 2025 to 30 April 2026.

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 GatewayAPI, 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, 27 May 2026

BDO Statsautoriseret revisionspartnerselskab

Nicolai T. Visti
Partner, Statsautoriseret revisor

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

2. ONLINECITY GROUP APS' STATEMENT

ONLINECITY Group ApS offers SMS gateways as a Software-as-a-Service (SaaS) solution according to a contract with
municipalities and private businesses. The SMS gateways are systems for sending and receiving SMS.
The accompanying description has been prepared for ONLINECITY Group ApS' customers and their auditors, who have a sufficient understanding to consider GatewayAPI 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.

ONLINECITY Group ApS uses subservice providers. This subservice provides relevant control objectives and related technical and organisational measures, and other controls are not included in the accompanying description.

ONLINECITY Group ApS confirms that the accompanying description in section 3 fairly presents GatewayAPI and the related controls for the period 1 May 2025 to 30 April 2026. The criteria used in making this statement were that the accompanying description:

1. Accounts for the GatewayAPI, and how the related controls were designed and implemented, including accounts for:
    - The types of services provided, including processed groups of transactions, when relevant.
    - The processes in both IT systems and manual systems which are used to initiate, record, process and, if necessary, correct the transactions and transfer these to the reports prepared for customers.
    - The related accounting records, underlying information and specific accounts used to initiate, record, process and report transactions, including the correction of incorrect information, and how the information is transferred to the reports prepared for customers.
    - How the system processed other significant events and matters than transactions.
    - The process used to prepare reports to customers.
    - 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 service providers GatewayAPI during the period 1 May 2025 to 30 April 2026.

3. Does not omit or distort information relevant to the scope of GatewayAPI 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 GatewayAPI which the individual customer may consider of importance to their special environment.

ONLINECITY Group ApS confirms that the controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively for the period 1 May 2025 to 30 April 2026. 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.

Odense, 27 May 2026

ONLINECITY Group ApS

Thomas Richard Hofmann Chairman of the board	Birol Altinok Executive	Martin Eland Pløger Executive

3. ONLINECITY GROUP APS' DESCRIPTION OF GATEWAYAPI

GENERAL DESCRIPTION OF ONLINECITY GROUP APS

ONLINECITY Group ApS is a Danish-owned company, which develops and operates several online systems for municipalities and various industries in the private market. ONLINECITY Group ApS has offices in Odense and Copenhagen.

ONLINECITY Group ApS has approximately 50 employees who are specialised in system development, server operation, support and information security, and they are organised in a development department, an operations and support department, a finance department and an administration department.

The Compliance team and ONLINECITY Group ApS' Security Committee manages the personal data security in relation to the processing that ONLINECITY Group ApS performs on behalf its customers, such as making data processing agreements, responding to request from the Data Controller, notification of breach of the personal data security, compliance with internal policies and procedures, and similar areas.

In connection with the performance of our service, it may be necessary to make use of external assistance. We always ensure that agreements with external service providers and outsourcing suppliers are formalised, when relevant, and that business partners are familiar with our IT security policy.

Risk assessment
Management is responsible for implementing all initiatives that address the threat scenario which ONLINECITY Group ApS is facing from time to time, so that implemented security measures and controls are appropriate, and the risk of breach of the personal data security is reduced to an appropriate level.

On a yearly basis, ONLINECITY Group ApS 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 ongoing audits as part of the annual wheel, the risk assessments may form the basis for new projects, which are to increase the information security of all of ONLINECITY Group ApS' IT platforms.

This report includes solely controls and control objectives for processes and controls which are managed by ONLINECITY Group ApS and, thus, it does not include controls or control objectives, which are managed by subservice organisations.

CONTROL FRAMEWORK, CONTROL STRUCTURE AND CRITERIA FOR IMPLEMENTATION OF CONTROLS

ONLINECITY Group ApS' information security is defined on the basis of the objective of providing dedicated IT outsourcing and high-quality infrastructure solutions, including stability and security.

The determination of criteria and scope of the implementation of controls at ONLINECITY Group ApS 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 ONLINECITY Group ApS to customers, and they include control areas and control activities within operation and hosting. All of the above areas are separately described in detail 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

ONLINECITY Group ApS has implemented policies and procedures to ensure that ONLINECITY Group ApS is able to provide sufficient guarantees to complete appropriate technical and organisational security measures. ONLINECITY Group ApS has prepared and implemented an information security policy approved by Management, which is currently examined and updated.

A.5.2 Information security roles and responsibilities

ONLINECITY Group ApS has implemented controls to ensure a general regulation of information security, including delegation of responsibility and risk management in accordance with the requirements from the Company's Management.

ONLINECITY Group ApS ensures that the same person does not have access to enter, change or use systems, information or infrastructure, without approval, or else it would be detected.

A.5.3 Segregation of duties

ONLINECITY Group ApS's functions and duties are segregated, to the extent possible given the size of the organisation, in order to reduce the possibility of unauthorised or unintended use, change or misuse of data.

A.5.4 Management responsibility

Management takes active part of the IT security within the organisation. The formal responsibility, including the approval of the information security policy, falls also on the managing director.

A.5.9 Inventory of information and other associated assets

ONLINECITY Group ApS maintains a record of assets including employees' equipment. All assets are assigned to an owner.

A.5.15 Access control

ONLINECITY Group ApS has implemented controls to ensure that access to systems, data and network services is provided through a documented process in accordance with a relevant work-related need and is terminated when the relevant access is no longer necessary.

A.5.16 Identity management

ONLINECITY Group ApS has established a procedure for registering and deregistering users in connection with granting access rights.

A.5.17 Authentication information

ONLINECITY Group ApS has determined rules for password requirements, which must be followed by all employees and external consultants. The design of requirements for length, complexity, and password history, as well as account lockout after unsuccessful login attempts follows best practice for a secure logical access control. Technical measures supporting these requirements have been implemented. A procedure for clear desk and screen policy has been established, and enforced when workstations are left unattended. The requirement for the application of lock screen is described in the IT security policy,

A.5.18 Access rights

ONLINECITY Group ApS has established a procedure for granting, adjusting, and revoking access rights, including upon termination or resignation. All access rights are reviewed annually, and an access control report is conducted each year to ensure the appropriate allocation of user permissions. The company is adhering to the principle of least privilege, and access rights are granted, based on work-related needs.

A.5.19 Information security in supplier relationships
ONLINECITY Group ApS uses Google LLC and Hetzner Online GmbH as a subservice provider for backup. The service provided by Google and Hetzner includes:

- Hosting of servers
- Backup

ONLINECITY Group ApS has determined information security requirements for subservice providers used, and has limited the subservice provider's access to relevant systems and data in relation to the subservice provider's work-related needs.

A.5.20 Addressing information security within supplier agreements
ONLINECITY Group ApS has determined information security requirements to applied subservice providers in the service agreements entered.

A.5.22 Monitoring, review and change management of supplier services
ONLINECITY Group ApS performs annual supervisions of the subservice providers applied, including obtains and reviews the subservice provider's audit opinions, certifications and similar documents. Supervisions of subservice providers are performed at least once a year and are based on a risk assessment. An annual oversight report is conducted on our sub-processors, followed by a comprehensive evaluation.

A.5.23 Information security for use of cloud services.
ONLINECITY Group ApS has determined which information risks are connected to the use of cloud services. ONLINECITY Group ApS has processes for acquisition, use, control and termination of the use of cloud services in accordance with the organisation's information security requirement.

A.5.24 Information security incident management planning and preparation
ONLINECITY Group ApS has implemented a procedure for managing breaches of the information security, including allocating roles and responsibilities in connection to breaches of the information security. A contingency plan has been established and implemented to ensure the timely restoration of access to data and system availability in the event of a security breach.

A.5.37 Documented operation procedures.
ONLINECITY Group ApS has implemented operating procedures to ensure secure operation of information processing facilities. Operating procedures are available for all relevant personnel.

A.6: People controls
A.6.1 Screening
Before employment, sufficient screening of potential applicants is conducted, including obtaining criminal records where relevant. All personnel at ONLINECITY Group ApS have committed themselves to confidentiality by signing an employment contract, which includes terms and conditions relating to secrecy and confidentiality.

A.6.3 Information security awareness, education and training
New employees receive sufficient information on information security and GDPR upon employment and are required to review and acknowledge the information security policies and procedures.
ONLINECITY Group ApS conducts current, and at least once a year, awareness training in accordance with the information security policy and the management thereof. The annual awareness training consists of tests, and the result is used to evaluate the effectiveness of the training program, and identify areas for improvement in information security awareness.

A.6.7 Remote working
ONLINECITY Group ApS has implemented procedures to ensure that access from workplaces outside ONLINECITY Group ApS's premises and remote access to systems and data is via VPN-connections with two-factor authentication to systems with personal data. Access from workplaces outside ONLINECITY Group ApS

premises to all external services uses HTTPS, which ensures encryption and prevents leak of information which is accessed via the user's account with 2-factor-authentification.

A.6.8 Information security event reporting
ONLINECITY Group ApS has implemented procedures to ensure that any information security incidents and vulnerabilities are reported to relevant parties. Incidents are reported through the company's request form, and appropriate actions will be carried out based on the specific case.

A.7: Physical controls
A.7.1 Physical security perimeters
ONLINECITY Group ApS 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
ONLINECITY Group ApS' premises have access control in the form of a required code and a system key to ensure that only authorised staff has access. Only ONLINECITY Group ApS' employees will receive a key and a code. If suppliers, consultants or other external parties need access, then they are escorted during their visit.

A.8: Technological controls
A.8.2 Privileged access rights
The allocation and use of privileged access rights are limited and controlled. Privileged access rights are granted solely based on a work-related need.

A.8.3 Information access restriction
To prevent unauthorised access to information and supporting assets, access must be restricted to the greatest extent possible in accordance with ONLINECITY Group ApS' policy for access control.

A.8.4 Access to source code
To prevent unauthorised functionality or other harmful changes, access to source code is restricted based on a work-related need.

A.8.5 Secure authentication
ONLINECITY Group ApS has implemented procedures and measures to ensure that users are securely authenticated when accessing systems, applications and services.

A.8.7 Protection against malware
ONLINECITY Group ApS has put in place procedures to ensure that devices with access to networks and applications are protected from viruses and malware. Antivirus programs and other protection systems are updated and adjusted to the current threat level, and monitoring of these systems is set up, including periodic testing for functionality.

A.8.8 Management of technical vulnerabilities
ONLINECITY Group ApS has implemented policies and procedures in regards to management of vulnerabilities. Identified vulnerabilities are evaluated subsequently and managed with appropriate initiatives. An annual pentest is conducted on the GatewayAPI platform annually, and findings shall be evaluated and appropriate actions must be taken, to address the identified vulnerabilities.

A.8.9 Configuration management
ONLINECITY Group ApS has implemented procedures to enforce and manage the defined configurations regarding security settings for hardware, software, services and networks.

A.8.13 Information backup
ONLINECITY Group ApS has implemented procedures to ensure that backup is taken of systems and data to prevent loss of data or loss of accessibility in case of crashes. Backups are kept at an alternative location. Backups are protected by physical and logical security measures to prevent that data falling into the hands of third parties, or that backups are destroyed by fire, water, vandalism, or accidental damage.

A.8.15 Logging
ONLINECITY Group ApS has implemented procedures to ensure that logging has been set up in accordance with the requirements in legislation and business needs, based on a risk assessment of systems and the current threat scenario. The scope and quality of log data is sufficient to identify and prove a potential abuse of systems or data, and log data are examined for applicability and abnormal behaviours. Log data is protected against loss and erasure. User transactions, including successful and unsuccessful attempts of access, exceptions and security incidents, are logged, and the log is stored according to the retention periods agreed upon with the customer.

A.8.19 Installation of software on operational systems
The installation of third-party supplier services, including tools, applications, systems, software, or cloud services, must be requested through the internal request form. Access is granted upon approval of the request. ONLINECITY Group ApS has also established general requirements for installation of software on workstations and servers. This includes ensuring the integrity of test and production systems and preventing exploitation of technical vulnerabilities.

A.8.20 Networks security
ONLINECITY Group ApS has implemented controls to ensure that the operation of material infrastructure components is performed in a structured and secure manner. ONLINECITY Group ApS has written documentation for configuration of firewalls, routers and switches, which are solely performed by the operations department.

A.8.21 Security of network services
ONLINECITY Group ApS has implemented procedures to ensure that traffic between the internet and the network is controlled by a firewall. Access from the outside via ports in the firewall is limited as much as possible and access rights are allocated via specific ports to specific segments.

A.8 22 Segregation of networks
ONLINECITY Group ApS has implemented procedures to ensure that networks in relation to use and security are divided into several virtual networks (VLAN), in which traffic between the individual networks is controlled by a firewall. Servers with an integrated firewall use this to ensure that access is given only to the necessary services.

A.8.29 Security testing in development and acceptance
ONLINECITY Group ApS has implemented a procedure for Secure Development, and ensures that information security is an integral part of the development lifecycle. When developing new information systems, requirements for information security are incorporated as early as possible, after which security testing is performed to ensure the necessary information security.

A.8.30 Outsourced development
When using external suppliers and general outsourcing to system development activities, ONLINECITY Group ApS conducts ongoing supervision and monitoring of the supplier's services.

A.8.31 Separation of development, test and production environments
Development, test and production environments are separated, and duties are segregated between the employees in the development department and in the operations and support department. Each development and change task go through a test run, and production data is never used as test data. Procedures have been introduced for version control, logging and backup, so that it is possible to reinstall previous versions.

Regardless of the nature of the change, it is ensured, as a minimum, that:

- All changes are prioritised and approved
- All changes are approved before commencement of operation
- All changes are put into operation on a fixed date outside of normal working hours
- Fall-back planning is conducted to ensure that changes can be rolled back or cancelled, should they not work
- System documentation is updated with the most recent change, if deemed necessary.

A.8.32 Change management

ONLINECITY Group ApS has a formal change management procedure in place to ensure that the systems are reviewed and tested in connection with bigger changes and is used to manage development. Tasks follow a uniform process, which starts with a risk assessment in accordance with the defined requirements. Security patches are applied in alignment with the patch management procedure and according to the supplier's recommendations.

Changes in the period 1 May 2025 to 30 April 2026

ONLINECITY Group has not made any significant changes to the GatewayAPI products' functionalities in the period from 1 May 2025 to 30 April 2026.

COMPLEMENTARY CONTROLS AT THE CUSTOMER

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:

- It is the responsibility of the customer to ensure that the administrators' use of the platform is in accordance with relevant legislation.
- The customer manages the user rights in the platforms, including to whom administrators' access is allocated and which rights are allocated 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 ONLINECITY Group ApS' description of GatewayAPI 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 ONLINECITY Group ApS, 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 2025 to 30 April 2026.

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 ONLINECITY Group ApS 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 Google Cloud Web Hosting within Hosting we have received SOC 2 report for the period from 1. November 2024 to 31. October 2025, and ISO 27001 certificate for the sub-processor's technical and organisational security measures and other controls.

For the services provided by Hetzner Online GmbH within Hosting, we have received an updated TÜV report and ISO 27001 certificate for the sub-processor's technical and organisational security measures and other controls.

These subservice providers' relevant control objectives and related controls are not included in ONLINECITY Group ApS' description of GatewayAPI and the related controls. Accordingly, we have only inspected the documentation received and tested the controls at ONLINECITY Group ApS, which ensure monitoring of the subservice provider's fulfilment of the agreement entered between the subservice provider and ONLINECITY Group ApS.

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 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 that the service provider has carried out a risk assessment based on potential risks to the availability, confidentiality and integrity of data. We have inspected that risks are minimised based on the assessment of their probability, consequences and derived implementation costs. We have inspected that the risk assessment carried out has been updated and approved.	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.	▶ The service provider has established and implemented an information security policy. ▶ The service provider's information security policy is reviewed and updated at least once a year.	We have made inquiries with relevant personnel. We have inspected that there is an information security policy that the management has processed and approved. We have inspected documentation that the information security policy has been communicated to relevant stakeholders, including the service provider's employees. We have inspected that procedures have been updated and approved during the declaration period.	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.	▶ The service provider ensures that the same person is not authorised to access, modify and apply systems, information or infrastructure without approval or without it being detected. ▶ The service provider has a clear division of the organisation regarding information security and has detailed descriptions of responsibilities and roles for each individual employee.	We have made inquiries with relevant personnel. We have inspected that there is an information security policy that the management has processed and approved. We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases. We have inspected that the service provider has assessed and approved user access during the declaration period.	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,	We have made inquiries with relevant personnel.	No exceptions noted.

	to reduce the possibility of unauthorised or unintentional use, modification or misuse of data.	We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases. We have inspected that the service provider has assessed and approved user access during the declaration period. We have inspected that privileged access rights solely are provisioned to employees with a work-related need.	
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 ensures that all employees and relevant suppliers are informed and maintain the service provider's requirements for information security.	We have made inquiries with relevant personnel. We have inspected that the service provider provides awareness training to employees. We have inspected documentation that all employees have completed the training offered.	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.	▶ The service provider maintains a list of assets used to perform the service provider's activities (this includes employee equipment). ▶ Used assets are assigned to an owner.	We have made inquiries with relevant personnel. We have inspected that the service provider maintains a list of assets used to perform the service provider's activities. We have inspected that both equipment and software are assigned owners.	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.	▶ The service provider has established a procedure for access control, which manages registrations and deregistrations of user access. ▶ The service provider has only granted employees access to the network and network services which they are authorised to use.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases. During the declaration period, we have inspected that the employee's access to systems has been approved and that the employees have a work-related need for the access.	No exceptions noted.

		During the declaration period, we have inspected to the resigned employees to ensure that their resigned's access to systems and databases has been deactivated or discontinued in due time. We have inspected that the service provider has assessed and approved user access during the declaration period.	
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 that formalised procedures are in place for granting and discontinuing users' access to systems and databases. During the declaration period, we have inspected that the employee's access to systems has been approved and that the employees have a work-related need for the access. During the declaration period, we have inspected to the resigned employees to ensure that their resigned's access to systems and databases has been deactivated or discontinued in due time.	No exceptions noted.
Authentication information To ensure proper entity authentication and prevent failures of authentication processes, according to to ISO/IEC 27002 A.5.17.	▶ The service provider has established rules for password requirements which must be followed by all employees as well as external consultants. ▶ The service provider has established systems for password management, and these are active. ▶ 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 that the service provider has established rules for password requirements which must be followed by all employees. We have inspected that users' access is done through passwords that reflect the risk of the processing activity. We have inspected that the service provider has established logical access control to systems, including the use of two-factor authentication.	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.	▶ The service provider has established a procedure for access control of allocation and revocation of access rights ▶ The service provider conducts periodic reviews of user access rights. ▶ The service provider revokes and adjusts access rights, when an employee resigns or an agreement expires.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases. During the declaration period, we have inspected that the employee's access to systems has been approved and that the employees have a work-related need for the access. During the declaration period, we have inspected to the resigned employees to ensure that their resigned's access to systems and databases has been deactivated or discontinued in due time. We have inspected that the service provider has assessed and approved user access during the declaration period.	No exceptions noted.
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 sub-service 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 that the service provider has established information security requirements to sub-service providers used. We have been informed that the sub-service provider does not have access to the service providers systems.	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 that the service provider has established information security requirements to sub-service providers used. We have inspected that the information security requirements are agreed upon.	No exceptions noted.

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 service provider performs supervision, which includes obtaining and reviewing the subservice provider's audit opinions, certifications, etc. ▶ The service provider performs supervision of subservice providers based on a risk assessment. ▶ The service provider performs supervision of subservice providers at least once a year, based on a risk assessment. ▶ The service provider assesses any changes to supplier services.	We have made inquiries with relevant personnel. We have inspected that the service provider has carried out supervision, including obtaining and reviewing the sub-service provider's auditor's statements, certifications and the like. We have inspected that the service provider's supervision of sub-processors has not given rise to any further action.	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.	▶ The service provider has determined which information risks are connected by using cloud services. ▶ The service provider has processes for acquisition, use, managing and termination of the use of cloud services in accordance with the organisation's information security requirements. ▶ The service provider has defined which information security measures that are managed by the provider of cloud services, and which are managed by the service provider in connection with the use of cloud services.	We have made inquiries with relevant personnel. We have inspected that the service provider has determined which information risks are connected by using cloud services. We have inspected that cloud sub-service providers have the same information security requirements as the service provider.	No exceptions noted.
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.	▶ Management responsibility and roles in connection with breaches of information security are determined.	We have made inquiries with relevant personnel. We have inspected that the service provider has implemented a procedure for managing breaches of the information security.	No exceptions noted.

	▶ The service provider has implemented a procedure for managing breaches of the information security.	We have inspected that the service provider provides awareness training to employees in relation to the identification of any data breaches. We have inspected that the service provider has established a contingency plan and that it has been tested during the 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 that operating procedures have been made available for 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.	▶ The service provider performs screening of potential employees before employment.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure the performance of screening and background checks of the service provider's employees in connection with employment. We have randomly inspected that the service provider has carried out verification of candidates before employment, and that the checks have included relevant documentation.	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 service provider conducts awareness training for new employees upon employment in accordance with the information security. ▶ Introduction courses regarding information security are conducted for new employees. ▶ The service provider performs current awareness training and quizzes for employees in accordance with the information security and the management thereof.	We have made inquiries with relevant personnel. We have inspected that the service provider is conducting an introductory course for new employees. We have inspected that the service provider conducts ongoing awareness, training and education of employees covering general IT security. We have inspected documentation that all employees have completed the training offered.	No exceptions noted.
Remote working To ensure information security when employees are working remotely, according to ISO/IEC 27002 A.6.7.	▶ Antivirus software must be installed and updated on all mobile devices used for work purposes.	We have made inquiries with relevant personnel. We have randomly inspected that for employees' PCs, antivirus has been installed that has been updated.	No exceptions noted.

	▶ Remote access to the service provider's systems and data takes place through an encrypted VPN connection. ▶ Remote access must be conducted through two-factor authentication.	We have inspected the service provider's network topology and observed that remote access to systems and data can only be achieved through VPN. We have inspected documentation that the service provider's network is set up in accordance with the network topology. We have inspected documentation that access to the VPN connection is done via appropriate security measures.	
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 that the service provider has an overview of security incidents with an indication of whether the individual incident has resulted in a breach of data security. We have inspected that all registered breaches of data security at the service provider have been notified to the relevant parties.	No exceptions noted.

A.7 Physical controls			
Control objective	**Control activity**	**Test performed by BDO**	**Result of test**
Physical security perimeters To prevent unauthorised physical access, damage and interference to the organisation's information and other associated assets, according to ISO/IEC 27002 A.7.1	▶ Physical security perimeters have been established to protect areas containing sensitive and critical information.	We have made inquiries with relevant personnel. We have inspected that physical security perimeters have been established. We have inspected that formalised procedures are in place to ensure that only authorised persons can gain physical access to the service provider's premises.	No exceptions noted.
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.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place to ensure that only authorised persons can gain physical access to the service provider's premises. We have inspected documentation that only authorised persons have physical access to premises. We have inspected overview of keys to the service provider’s premises.	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.	▶ Privileged (administrative) access rights to software, systems and devices are allocated based on work-related needs.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases. During the declaration period, we have inspected that the employee's privileged access to systems has been approved and that the employees have a work-related need for the privileged access.	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.	▶ The service provider has restricted the employees' and customers' access to information, based on work-related needs and applicable contracts with customers.	We have made inquiries with relevant personnel. We have inspected that formalised procedures are in place for granting and discontinuing users' access to systems and databases. During the declaration period, we have inspected that the employee's access to systems has been approved and that the employees have a work-related need for the access.	No exceptions noted.
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.	▶ Access to source code is restricted to relevant users.	We have made inquiries with relevant personnel. We have inspected that only the data processor's developers have access to source code. We have inspected documentation that the source code is protected against unauthorized modification and deletion.	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.	▶ The service provider has established logical access control to systems with information, including two-factor authentication.	We have made inquiries with relevant personnel. We have inspected that the service provider has established logical access control to systems, including the use of two-factor authentication.	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.	▶ Controls have been implemented for detection, prevention and recovery combined with suitable user awareness to protect against malware.	We have made inquiries with relevant personnel. We have randomly inspected that for PCs, antivirus has been installed and that the antivirus has been updated.	No exceptions noted.
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 vulnerability management procedure. We have inspected randomly selected vulnerability scans and observed that there are not critical or high vulnerabilities. We have inspected that the service provider has conducted a penetration test.	No exceptions noted.
Configuration management To ensure that hardware, software, services and networks function correctly with the required security settings, and that configuration is not altered by unauthorised or incorrect changes, according to ISO/IEC 27002 A.8.9.	▶ The service provider ensures that hardware, software, services and network functions correctly in relation to the security measures, which are pre-defined and ensure that these configurations cannot be changed.	We have made inquiries with relevant personnel. We have inspected by extraction that databases and networks are updated with relevant updates and security patches. We have randomly inspected that a workstation is updated with the latest system update.	No exceptions noted.

Information backup To enable recovery from loss of data or systems, according to ISO/IEC 27002 A.8.13.	▶ Backup of systems and data is performed daily. ▶ Storage of backup is outsourced to the subprocessor. ▶ A restore test is performed 1 time a year.	We have made inquiries with relevant personnel. We have inspected that formalized procedures are in place to ensure daily backup and restoration of relevant data and systems, and that backups are stored in another physical location. We have inspected that backups of relevant systems and data are made in accordance with the procedure. We have inspected that backups have been restored during the declaration period.	No exceptions noted.
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.	▶ All successful and unsuccessful attempts to access the service provider's systems and data are logged. ▶ All user changes in systems and databases are logged. ▶ The service provider has set up restrictions for who may get access to log data. ▶ The service provider logs activities by administrators and operators. ▶ The log is deleted after the agreed-upon retention period. ▶ The service provider stores logs for 30 days.	We have made inquiries with relevant personnel. We have inspected that logging of user activities in systems, databases and networks is configured and enabled. We have inspected user changes are logged. We have inspected that collected information about user activity in logs is protected from manipulation and deletion. We have inspected that only authorized personnel can access logs. We have inspected that there are alarms on logs. We have inspected that logs are deleted after 30 days.	No 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.	▶ The service provider has implemented procedures for installation of software installation. ▶ The service provider has introduced rules for installation of software.	We have made inquiries with relevant personnel. We have inspected that the service provider has implemented procedures for installation of software installation. We have inspected the request flow of installing software for employees.	No exceptions noted.
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 cannot be accessed directly from the internet. ▶ 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 networks are segmented in order to ensure limited access to systems and databases. We have inspected documentation that the service provider's network is set up in accordance with the network topology.	No exceptions noted.
Security of network services To ensure security in the use of network services, according to ISO/IEC 27002 A.8.21.	▶ The service provider has implemented/set requirements for suitable security measures to protect its network services.	We have made inquiries with relevant personnel. We have inspected the service provider's network topology and observed that networks are segmented in order to ensure limited access to systems and databases. We have inspected documentation that the service provider's network is set up in accordance with the network topology.	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.	▶ The service provider's network is segregated so that internal servers cannot communicate directly with the internet.	We have made inquiries with relevant personnel. We have inspected the service provider's network topology and observed that networks are segmented in order to ensure limited access to systems and databases. We have inspected documentation that the service provider's network is set up in accordance with the network topology.	No exceptions noted.
Security testing in development and acceptance To validate if information security requirements are met when applications or code are implemented in the production environment, according to ISO/IEC 27002 A.8.29.	▶ Information security requirements and requirements for the processing of information are included in an early assessment of projects/systems. ▶ The service provider has implemented security measures for information which goes through the public network.	We have made inquiries with relevant personnel. We have inspected that the service provider has established a procedure for development and modification tasks that ensures that all development and modification tasks follow a formalized process that ensures testing and requirements for approval before implementation. We have randomly inspected for implemented changes that the tasks have followed the formalised process, and that tests have been carried out and that the changes have been approved before implementation.	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.	▶ Segregation of duties between development and production is implemented. ▶ Changes of functionality are tested before they are put into service. ▶ Development and test are performed in development environments, which are segregated from production systems.	We have made inquiries with relevant personnel. We have inspected that the development, testing and production environment are separated. We have inspected that the service provider has established a procedure for development and modification tasks that ensures that all development and modification tasks follow a formalized	No exceptions noted.

	▶ A version control system is used to register all changes to the source code. ▶ Development and test environments are segregated.	process that ensures testing and requirements for approval before implementation. We have randomly inspected for implemented changes that the tasks have followed the formalised process, and that tests have been carried out and that the changes have been approved before implementation.	
Change management To maintain information security when executing changes, according to ISO/IEC 27002 A.8.32.	▶ The service provider has established procedures for change management. ▶ The service provider has established procedures for system changes. ▶ The service provider performs suitable tests of new systems and system changes. ▶ The service provider has established rules to limit software installations.	We have made inquiries with relevant personnel. We have inspected that the service provider has established a procedure for development and modification tasks that ensures that all development and modification tasks follow a formalized process that ensures testing and requirements for approval before implementation. We have randomly inspected for implemented changes that the tasks have followed the formalised process, and that tests have been carried out and that the changes have been approved before implementation. We have inspected that the service provider has implemented procedures for installation of software installation. We have inspected the request flow of installing software for employees.	No exceptions noted.

BDO STATSAUTORISERET REVISIONSPARTNERSELSKAB

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."

Martin Eland Pløger
Executive
Serienummer: 920bff87-27da-4280-8d09-3f4383fc2b82
IP: 185.229.xxx.xxx
2026-05-29 08:13:38 UTC

Mit ID

Birol Altinok
Executive
Serienummer: 14a524ff-0318-45f4-9755-75fa8e5c965d
IP: 152.115.xxx.xxx
2026-05-29 08:28:21 UTC

Mit ID

Thomas Richard Hofmann
Chairman of the board
Serienummer: 92543bc8-b721-487f-acd5-3044efd86591
IP: 80.208.xxx.xxx
2026-06-01 10:00:19 UTC

Mit ID

Nicolai Tobias Visti Pedersen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Statsautoriseret revisor
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: c42f66e9-59bb-478a-9d92-2a2b8602724e
IP: 37.96.xxx.xxx
2026-06-01 11:22:13 UTC

Mit ID

Mikkel Jon Larssen
BDO Statsautoriseret Revisionspartnerselskab CVR: 45719375
Partner
På vegne af: BDO Statsautoriseret Revisionspartnerse…
Serienummer: cd9a38dd-e75c-40f7-80d6-ec5b5d0841d6
IP: 77.243.xxx.xxx
2026-06-01 16:07:35 UTC

Mit ID