Curanet A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2024 to 31 December 2024 in relation to Curanet A/S's hosting services to customers

March 2025

Contents

1. Management's assertion 3

2. Independent service auditor's assurance report on the description, design and operating effectiveness of controls 5

3. System description 8

4. Control objectives, control activity, tests and test results 18

1. Management's assertion

The accompanying description has been prepared by Curanet A/S (Curanet) for customers who have used the hosting services and their auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements in their financial statements.

Curanet uses Fuzion A/S and GlobalConnect A/S as subservice suppliers of housing; Cibicom A/S as a subservice supplier of housing and storage of backup; B4Restore A/S as a subservice supplier of backup and an EDR/XDR subservice provider as a subservice supplier of cloud storage and reporting logic for a subset of logging and monitoring on critical platforms. This report uses the carve-out method, and the description in section 3 includes only the controls and related control objectives of Curanet and excludes the control objectives and related controls of Fuzion A/S, GlobalConnect A/S, Cibicom A/S, B4Restore A/S and an EDR/XDR subservice provider. Our evaluation did not extend to controls of Fuzion A/S, GlobalConnect A/S, Cibicom A/S, B4Restore A/S and an EDR/XDR subservice provider.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of our controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Curanet confirms that:

a) The accompanying description in section 3 fairly presents the hosting services that have processed customers' transactions throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

(i) Presents how IT general controls in relation to the hosting services were designed and implemented, including:

- The types of services provided
- The procedures, within both information technology and manual systems, by which the IT general controls were managed
- Relevant control objectives and controls designed to achieve those objectives
- Controls that we assumed, in the design of the hosting services, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
- How the system dealt with significant events and conditions other than transactions
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to IT general controls

(ii) Includes relevant details of changes to IT general controls in relation to the hosting services during the period from 1 January 2024 to 31 December 2024

(iii) Does not omit or distort information relevant to the scope of IT general controls in relation to the hosting services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of IT general controls in relation to the hosting services that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2024 to 31 December 2024. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified;

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2024 to 31 December 2024.

Skanderborg, 5 March 2025
Curanet A/S

Lotte Bendstrup
MD

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2024 to 31 December 2024 in relation to Curanet's hosting services to customers

To: Curanet A/S (Curanet), its customers and their auditors

Scope

We have been engaged to report on Curanet's description in section 3 of IT general controls in relation to the hosting services which have processed customers' transactions throughout the period from 1 January 2024 to 31 December 2024 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Curanet uses Fuzion A/S and GlobalConnect A/S as subservice suppliers of housing; Cibicom A/S as a subservice supplier of housing and storage of backup; B4Restore A/S as a subservice supplier of backup and an EDR/XDR subservice provider as a subservice supplier of cloud storage and reporting logic for a subset of logging and monitoring on critical platforms. This report uses the carve-out method, and the description in section 3 includes only the controls and related control objectives of Curanet and excludes the control objectives and related controls of Fuzion A/S, GlobalConnect A/S, Cibicom A/S, B4Restore A/S and an EDR/XDR subservice provider. Our evaluation did not extend to controls of Fuzion A/S, GlobalConnect A/S, Cibicom A/S, B4Restore A/S and an EDR/XDR subservice provider.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of Curanet's controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Curanet's responsibilities

Curanet is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

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

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of Curanet's description and on the suitability of the design and operation of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3402, “Assurance Reports on Controls at a Service Organisation”, issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description of a service organisation’s system and the suitability of the design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the description and the design and operating effectiveness of controls. The procedures selected depend on the service auditor’s judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by Curanet and described in section 1.

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

Inherent limitations

Curanet’s description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the hosting services that the individual customer may consider important in its own particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in the hosting services. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria including the control objectives described in Curanet’s assertion in section 1:

a) The description fairly presents how IT general controls in relation to the hosting services were designed and implemented throughout the period from 1 January 2024 to 31 December 2024;

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2024 to 31 December 2024 and user entities applied the complementary customer controls referred to in section 3; and

c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2024 to 31 December 2024.

Description of test of controls

The specific controls tested and the nature, timing and results of these tests are listed in section 4.

Intended users and purpose

We were engaged to report by Curanet and, therefore, this report and the description of tests of controls and results thereof in section 4 are intended for the use of Curanet.

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Curanet, at its discretion, to customers who have used Curanet's hosting services during some or all of the period of 1 January 2024 to 31 December 2024 and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

Our report is not to be used for any other purpose or to be distributed to any other parties.

Aarhus, 5 March 2025
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

3. System description

3.1. Introduction

This description is designed to provide information for the use of Curanet A/S's clients and their auditors and to meet the requirements of audit standard ISAE 3402, "Assurance Reports on Controls at a Service Organisation".

The description is also prepared with the aim of providing information on the controls used in relation to the provision of hosting services and IT operating services provided by Curanet A/S (Curanet).

3.2. Description of Curanet's services

Curanet develops, manages and delivers a range of professional hosting and cloud solutions for a wide range of companies and organisations in Denmark.

The scope of this assurance report covers the following services:

- Hosted Navision
- Hosted Desktop (Citrix)
- Hosted Exchange
- Mail hotel
- Web hotel
- Hosted Webshop
- Hosted CMS
- OnPay
- DNS Hotel and DNS servers' hosting domains
- Hosted Spam filter
- Veeam Backup.

Services not specifically mentioned above are not covered, but the infrastructure components (network, storage, management, operating systems) supporting the services are covered.

For the following products, only the infrastructure components (network, storage, management, hypervisor) are covered:

- Cloud Resource Pool (CRP)
- Virtual Data Center (VDC)
- Cloud Server
- VPS Hosting.

FlexVPS, Microsoft 365 and Azure services are also not covered.

3.3. Curanet's organisation and security

Curanet operates an ISO 27001-certified information management system. Information security is governed by the Security Board, which sets the overall objectives of the ISMS. The Security Board is composed of the following members:

- MD, Lotte Bendstrup
- CTO, Ole P. Jensen
- Group CISO, Jakob Flink Schwartz
- General Counsel, Lasse Lindberg Mortensen
- CISO Nordics, Jonas Beier Jørgensen.

The CISO Nordics refers to the Group CISO.

The group meets quarterly and on an ad hoc basis to set and follow up on IT security objectives and risks.

Risk management at Curanet

Risk management is implemented in Curanet as an integral part of Curanet’s processes. A risk register is continuously maintained throughout the year, containing the most significant risks to Curanet’s operation of services. Risk treatment plans are defined and tracked for risks that fall outside our risk acceptance criteria. The risk register is reviewed at least annually and approved by the Security Board.

3.4. Control framework, control structure and control implementation criteria

Curanet’s IT security policy established processes, and controls include all systems and services offered to customers. The continued work on adapting and improving Curanet’s security measures is ongoing in cooperation with highly qualified specialists.

The criteria and scope of the control implementation at Curanet were established in 2020 on the basis of the ISO 27001 and ISO 27002 standards. Based on this control framework, relevant control areas and control activities are implemented on the services provided by Curanet.

The following essential control areas shall be included in the overall control environment:

- Policies for information security (5.1)
- Access rights (5.18)
- Monitoring, review and change management of supplier services (5.22)
- Information security during disruption (5.29)
- Privileged access rights (8.2)
- Secure authentication (8.5)
- Capacity management (8.6)
- Management of technical vulnerabilities (8.8)
- Configuration management (8.9)
- Information backup (8.13)
- Logging (8.15)
- Security testing in development and acceptance (8.29)
- Change management (8.32).

3.5. Established control environment

Each area is described in detail in the following sections.

Policies for information security (5.1)

Objective

A Management-approved information security policy is based on an IT risk analysis and is communicated to relevant employees in the company.

Procedures and controls used

Curanet identifies relevant IT risks on established services to customers. This is done through an ongoing risk assessment at Curanet. The risk assessment is approved annually by the Security Board.

The information security policy is available for all employees and communicated to all employees at least annually. Other material changes are communicated on an ad hoc basis.

Timing of the control

The IT risk analysis and IT security policy are reviewed at least annually. The information security policy is communicated annually.

Who performs the control?

The risk assessment and the annual review of policies are approved by the Security Board.

Control documentation

The information security policy and the risk assessment are versioned, and the Security Board has approved them. Minutes of Security Board meetings are kept.

Access rights (5.18)

Objective

To ensure authorised user access and to prevent unauthorised access to systems and services.

Procedures and controls used

A formal process ensures new users are provisioned based on manager's approval. Access rights are based on access profiles related to their job function.

A formal process ensures that users' access rights are revoked, and users are disabled or deregistered upon termination of employment or contract.

A biannual review of users ensures that any inactive users or users without a work-related need for the privileges are removed.

Timing of the control

The user creation check is made whenever Curanet appoints a new employee. User deregistration is done when an employee is leaving Curanet. Checks on inactive users are carried out biannually.

Who performs the control?

The operations department of Curanet is responsible for compliance with the access procedures.

Control documentation

Documentation on registration, deregistration and reviews of users are kept in Curanet's internal ticketing system.

Monitoring, review and change management of supplier services (5.22)

Objective

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

Procedures and controls used

Conduct review of independent auditor's reports, if available, and assess issues identified. Conduct physical inspection of supplier services in data centres.

Timing of the control

The review of the suppliers' audit reports and the review of the suppliers' services are performed annually.

Who performs the control?

CISO and Infrastructure.

Control documentation

Documented review of supplier audit reports is stored in the internal documentation system. Documented review of supplier services is stored in the internal ticketing system.

Information security during disruption (5.29)

Objective

Planning for resuming business and services after any type of major incident.

Procedures and controls used

[Service organisation] has established a contingency plan which generally sets out guidelines on how to deal with any type of emergency situation. The contingency plan is approved annually by [Service organisation]'s Management.

The contingency plan is reviewed on an ongoing basis and at least once a year.

Timing of the control

The contingency plan is reviewed and approved annually.

Who performs the control?

The Information Security department is to review, and Management is to approve.

Control documentation

The contingency plan is versioned. There is evidence of actions taken in connection with the 'dry run' of the contingency plan.

Privileged access rights (8.2)

Objective

To ensure only authorised users and services are granted privileged access rights.

Procedures and controls used

Privileged access rights are limited to employees at Curanet who have a work-related need.

Privileged access rights are given and granted on a strict need-to-use basis based on employees' functional roles and must be approved by the manager.

A formal process ensures that privileged access rights are revoked when no longer required.

A biannually review of users ensures that any inactive users or users without a work-related need for the privileges are removed.

Timing of the control

Privileged access is assigned upon formal approval by the manager and is reviewed biannually to ensure continued relevance. Revocation occurs when the user no longer requires privileged access.

Who performs the control?

The operations department of Curanet is responsible for compliance with the access procedures.

Control documentation

Documentation is kept in Curanet's internal ticketing system.

Secure authentication (8.5)

Objective

To prevent unauthorised access to systems and applications.

Procedures and controls used

Access to Curanet's assets happens through a secure logon process. Users are stored in a central user database. Password requirements and lockout procedures are handled by the internal Windows Active Directory. Password and lockout settings are based on Curanet's risk assessment.

All access from external or untrusted networks requires MFA.

Timing of the control

User verification happens at logon.

Who performs the control?

Curanet's internal Windows Active Directory.

Control documentation

Logins are logged. Group policies and MFA system configuration.

Capacity management (8.6)

Objective

To ensure correct and secure operations of information processing facilities by ensuring availability of systems and services.

Procedures and controls used

Servers are monitored for availability on predefined services based on the categorisation and the type of the server. Alerts are raised when service checks fail and are handled by operations staff. Repetitive alerts are escalated for further root cause analysis.

Timing of the control

Services are checked every five minutes. A summary of repetitive alerts is generated daily.

Who performs the control?

Monitoring system checks services. Repetitive alerts are checked by operations staff.

Control documentation

Alerts are logged in the operations management system.

Management of technical vulnerabilities (8.8)

Objective

To prevent exploitation of technical vulnerabilities through patch management.

Procedures and controls used

For operating systems, Windows and Linux servers, security patches are installed continuously throughout the year, and exceptions are documented.

For hypervisors, security patches are evaluated by the system owner and installed appropriately.

For hardware devices, security patches are evaluated by the system owner and installed appropriately.

Timing of the control

The update check is automated through the respective patch platforms.

Who performs the control?

The operations department is responsible for carrying out updates and checking them.

Control documentation

Documented in the patch management platform. On each server, a list of patches installed is available.

Evaluated patches are documented in tickets.

Configuration management (8.9)

Objective

To ensure correct and secure operations of information processing facilities by ensuring that customers' servers are deployed according to our security baseline.

Procedures and controls used

Customers' servers are deployed based on our configuration baseline. This includes requirements for automatic patching, firewall settings and password policy.

Configuration baselines are reviewed at least annually.

Timing of the control

When customers' servers are deployed. Review of baseline is performed annually.

Who performs the control?

Deployment is automated by the deployment system. Review is done via peer review.

Control documentation

Deployment is logged in the deployment system, and the peer review is documented in an internal ticket.

Information backup (8.13)

Objective

To protect against loss of data for systems within Curanet's responsibility.

Scope

The scope of the report covers public systems providing services to customers where backup is included, i.e., Hosted Exchange, Web hotel, Hosted Desktop, Hosted Navision, VPS Server.

Internal systems providing services internally, i.e., corp. email, CMDB, intranet, management systems.

Operation of the IBM Spectrum (TSM) service is outsourced to B4Restore. Curanet still handles configuration and monitoring of backup jobs, and the service is still housed at Curanet-operated data centre sites. Therefore, this has not affected the controls in section 4.

Out of scope:

- Services without backup included:
    - Virtual servers: Cloud Server, Cloud Resource Pool (CRP), Virtual Data Centre (VDC)
    - Backup services provided where the customer manages the backup jobs and monitors backup jobs
    - Restore testing – We guarantee the integrity of our backup systems, but only the customer can test if their backup is valid.

Procedures and controls used

For "public systems providing services to customers", we guarantee backup of data with 14 days' retention and recovery point objective of 24 hours if there is no disruption to the backup job.

For "Internal systems providing services internally", we guarantee backup so they can be recovered again.

Backups are always stored in a different data centre than where production data is stored. Backup data is replicated to another data centre site daily.

The integrity of backup systems is continuously ensured by restore jobs internally and by customers.

We continuously test our restore capabilities by restoring internal systems and customer systems. Customers can order restore tests of their specific systems on an ad hoc basis.

There is an automated procedure for daily follow-ups on failed backup jobs. If a backup job fails consecutively two days in a row, a ticket is raised. If a backup job fails three times over a period of 14 days, a ticket is raised.

Timing of the control

Automatic backup has been established, and restore tests are carried out at least once a year.

Who performs the control?

The operations department is responsible for the day-to-day control of backup logs.

Control documentation

The backup log is stored in Curanet’s asset management system.

Logging (8.15)

Objective

To record events and generate evidence.

Procedures and controls used

Events from critical systems are logged to a central log management platform.

The Extended Detection and Response (XDR) platform logs and ships events off site for protection. The XDR platform monitors for malicious behaviour. Alerts are raised to operations staff for investigation.

Timing of the control

Continuously.

Who performs the control?

The operations team investigates events raised.

Control documentation

Logs are stored in the log management platform, and events are stored in the XDR platform.

Security testing in development and acceptance (8.29)

Objective

To validate if information security requirements are met when applications or code are deployed to the production environment.

Procedures and controls used

Changes to the operations management system are controlled and documented using:

- Version control to track modifications and maintain a history of changes
- Code reviews to ensure adherence to development standards and detect potential security vulnerabilities
- Static code analysis to identify security issues and vulnerabilities in the codebase before deployment.

Timing of the control

Security testing is performed during the development and acceptance phases of system changes, prior to deployment into the production environment.

Who performs the control?

The development and operations teams are responsible for implementing version control, conducting code reviews, and performing static code analysis as part of the development process.

Control documentation

Documentation of version control, code reviews and static code analysis results is maintained in the organisation's development and operations repositories (e.g., Git and other supporting systems).

Change management (8.32)

Objective

To ensure that planned changes to systems and services are controlled, documented and communicated in a consistent and standardised manner.

Procedures and controls used

- Planned changes are documented in accordance with a standardised process to ensure consistency and traceability.
- Maintenance announcements are made with all required information, including impact for customers, timeframe and a description of affected services.
- All maintenance announcements are processed and approved by the CTO.

Timing of the control

When changes are planned or executed.

Who performs the control?

The person planning or executing the change.

Control documentation

Changes to systems are registered and communicated to customers via the internal change announcement system.

Controls and implemented measures from ISO/IEC 27002:2022

A more detailed description of implemented measures appears in section 4 on the description of our control objectives and related controls as well as the auditor's description of the test of controls for this assurance report.

3.6. Subservice suppliers

team.blue Denmark uses the following as subservice supplier:

- Fuzion A/S for housing and physical and environmental security of production environment
- GlobalConnect A/S for housing and physical and environmental security of production environment
- Cibicom A/S for housing, physical and environmental security of production environment and storage of backup
- B4Restore A/S for IBM Spectrum (TSM) backup service
- An EDR/XDR subservice provider for cloud storage and reporting logic for a subset of logging and monitoring on critical platforms. For security reasons and in line with best practices, the vendor name is not disclosed.

3.7. Changes to Curanet's system during the period

During the reporting period, there were no changes to the design or operation of our system that would materially affect the suitability of the design and operating effectiveness of the controls in place to meet the stated control objectives.

3.8. Complementary controls at customers

Service delivery

The controls described in Curanet's system description is based on Curanet's standard terms. As a result, customer agreements which differ from Curanet's standard terms are not covered by the scope of this auditor's report. Customers and their auditors should assess whether the control scope in this auditor's report can be used in assessing the IT general controls at Curanet in relation to operations and hosting services provided from Curanet to the customer. Customers and their auditors should also themselves identify any other material risks related to their environment.

User management

Curanet provides access and assigns access privileges in accordance with customer instructions as they are registered through the Service Desk or Control Panels. Curanet is not responsible for the accuracy of information about users, and it is therefore the responsibility of customers to ensure that access and rights to systems and applications are allocated in accordance with the customers' own expectations for appropriate user management, including segregation of duties and periodic reassessment in the system environments hosted and operated by Curanet. If desired, the customer can create users on the individual servers themselves – controls related to this process are the responsibilities of the customers.

Logical security configuration

Curanet has configured logical security on its own infrastructure for providing operating and hosting services to its customers. Establishing and configuring logical security in customers' own environments are the responsibilities of the customers, and it is the responsibility of the customers to verify that these security configurations are consistent with the desired level of security.

Logging

Logging inside the customers' environments is the responsibility of the customers. Thus, each customer should ensure appropriate controls for configuration and monitoring of logs.

Backup

It is the customer's own responsibility to ensure that backup is set up according to the customer's own needs. Recovery of customer data from backup systems is only tested when a specific agreement has been concluded with the customer or if Curanet receives a request from the customer with a specific request. According to Curanet's procedures, it is subsequently the customer's responsibility to ensure that completed restore can be used as intended in the respective environments.

Contingency planning

Curanet has set up general contingency planning that includes Curanet's own infrastructure. Customers should therefore independently assess whether additional procedures or contingency plans need to be implemented, including verification thereof.

Compliance with relevant legislation

Curanet is not responsible for applications that are run on the hosted equipment. It is therefore the responsibility of customers to establish reassuring controls in the applications, including that they support compliance with the Danish Accounting Act, the Personal Data Act, the Financial Business Act and/or other relevant legislation.

4. Control objectives, control activity, tests and test results

4.1. Purpose and scope

We conducted our engagement in accordance with ISAE 3402, “Assurance Reports on Controls at a Service Organisation”, and additional requirements applicable in Denmark.

Our testing of the design, implementation and operational effectiveness of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2. Test actions

The test actions performed when determining the operating effectiveness of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned during the period from 1 January 2024 to 31 December 2024. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

4.3. Overview of control objectives, control activity, tests and test results

Control objective 5: Organisational controls

Objective: A Management-approved information security policy is based on an IT risk analysis and is communicated to relevant employees in the company.

No.	Curanet's control activity	Tests performed by PwC	Result of PwC's tests
5.1	*Policies for information security* Information security policies are documented and communicated to employees. Information security policies are reviewed and approved at least annually. An information security risk assessment of critical risks to Curanet's operations of infrastructure is documented, reviewed at least annually and approved.	Inspected that the information security policy and selected sub-policies are documented and available on the internal wiki. Inspected that the updated employee information security policy has been communicated to employees via the intranet. Inspected that the information security policy was reviewed and approved. Inspected the IT risk analysis and verified that it was updated in the audit period. Inspected that the IT risk analysis had been approved by the Security Board.	No exceptions noted.
5.18	*Access rights* Internal users at Curanet are created according to formal creation procedures based on a request from a manager. All internal users are created in the Windows domain with a personal user account. Periodic review of users with privileged access rights is performed, and inactive users as well as users without a work-related need for the access are removed. Internal users are disabled prior to or on the termination date of the employees.	Inspected that an access control policy covers the process and requirements for user access creations. Inspected on a sample basis that user creations are based on a ticket, and that the creation is requested and approved by a manager. Inspected on a sample basis that users with privileged access rights in the two Windows domains are reviewed in the audit period, and users without a work-related need for the access are removed. Inspected on a sample basis that terminated users' accounts are disabled according to the procedure.	No exceptions noted.

Control objective 5: Organisational controls

Objective: A Management-approved information security policy is based on an IT risk analysis and is communicated to relevant employees in the company.

No.	Curanet's control activity	Tests performed by PwC	Result of PwC's tests
5.22	*Monitoring, review and change management of supplier services* Curanet performs an annual review of independent auditor's reports for critical sub-suppliers, if available, and assesses issues identified. Curanet performs an annual physical inspection of supplier services in data centres, and the results are documented in the ticketing tool.	Inspected documentation showing that review of independent auditor's reports for critical sub-suppliers is performed and that the results are documented on the internal wiki. Inspected on a sample basis that annual physical inspection of supplier services in data centres was performed and documented in the ticketing tool.	No exceptions noted.
5.29	*Information security during disruption* A business continuity plan is documented, reviewed and annually approved by Management. Business continuity tests are conducted at least annually. There is evidence of actions taken in connection with the 'dry run' of the contingency plan.	Inspected that a business continuity plan is documented, and that it outlines the scope and implementation of the plan. Inspected that the business continuity plan has been reviewed annually and approved by Management in 2024. Inspected meeting notes and material used for the latest business continuity test performed and inspected that the test has been approved by the Security Board.	No exceptions noted.

Control objective 8: Technological controls

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Curanet's control activity	Tests performed by PwC	Result of PwC's tests
8.2	*Privileged access rights* Privileged access rights are limited to employees at Curanet with a work-related need.	Inspected the list of users with privileged access on the two internal Windows domains and per inquiry with key personnel verified that only users with a work-related need have access.	No exceptions noted.
8.5	*Secure authentication* Access to Curanet's network goes through secure logon in Windows Active Directory where the password is configured according to the formalised password policy. MFA is required for access from external networks.	Inspected the configuration of the password policy on the two internal Windows domains and verified whether it corresponded to the Management-approved password policy. Observed on a sample basis employees being validated through MFA.	No exceptions noted.
8.6	*Capacity management* All servers are automatically monitored for availability via the central monitoring tool. Alerts are pushed to the monitoring screens placed in the operations department.	Inspected for a sample of servers that availability monitoring is configured and verified whether deviations in availability are registered and any outages are handled. Observed that monitoring screens are placed in the operations department and verified with key personnel that alerts are monitored. Inspected that alarms are followed up on and documented.	No exceptions noted.
8.8	*Management of technical vulnerabilities* For operating systems, security patches for Windows and Linux servers are installed continuously throughout the year, and exceptions are documented. For hypervisors, security patches are evaluated by the system owner and installed appropriately.	Inspected that patch management policies were in place for Windows, Linux and VMWare ESXi and that they are up to date. Inspected on a sample basis that Linux and Windows servers had been updated throughout the audit period according to the patch policy. Inspected on a sample basis the ESXi patch level and verified via inquiry with key personnel that the patch level is in accordance with the patch policy.	No exceptions noted.

Control objective 8: Technological controls

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Curanet's control activity	Tests performed by PwC	Result of PwC's tests
8.9	*Configuration management* A yearly review of the configuration baseline is performed, and the review is approved by the line manager. New Windows servers that are created are configured in compliance with actual baselines defined in a number of scripts. This baseline contains specific requirements for password and patching.	Inspected documentation for the performed review of the configuration baseline and verified that the review was performed, peer reviewed and approved by the line manager. Inquired with key personnel on the procedure for creating a new VPS server with a Windows operating system. Observed whether a newly created Windows server is in compliance with the baseline.	No exceptions noted.
8.13	*Information backup* All Curanet services with backup included are stored for at least 14 days. Backup runs daily, and reoccurring errors result in a ticket to operations staff. Backup is stored off site away from any production system. Curanet performs restores for customers as part of the daily operations, and the customers are responsible for verifying that the integrity of the backup data is intact.	Inspected for selected server samples that backup retention is set to at least 14 days. For selected servers, Inspected that backup is performed on a daily basis and that backup errors result in a ticket that is handled according to the procedure. Inspected for selected server samples that backups are stored on different sites than production servers. Inspected documentation for one sample of a restore test performed in 2024 and verified that the results were approved by the client.	No exceptions noted.

Control objective 8: Technological controls

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Curanet's control activity	Tests performed by PwC	Result of PwC's tests
8.15	*Logging* Event logging is configured for Curanet's critical, central systems. Curanet's central critical logs are stored at an external party and cannot be altered. System administrator and system operator activities shall be logged in the operations management system.	Inspected on a sample basis that event logging is configured on two internal Windows domain controllers. Inspected whether the same two internal Windows domain controllers were also covered by EDR/XDR logging. Inspected on a sample basis that logs from two Windows domain controllers were transferred to the log management tool. Inquired of key personnel whether logs from server samples, Windows domain controllers and the operations management system are protected from deletion and manipulation. Inspected that a password access log from the operations management system for documenting the use of shared administrator users is available. Inspected on a sample basis whether user access logs are stored centrally.	No exceptions noted.
8.29	*Security testing in development and acceptance* Changes to Curanet's operations management system is controlled and documented through: • version control • code review • static code analysis.	Inspected the change management procedure and verified with key personnel that the process was valid in the audit period. Inspected for one sample that the system functionality supports version control as a standard. Inspected for selected change samples that code review and static code analysis are performed according to Curanet's requirements.	No exceptions noted.

Control objective 8: Technological controls

Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Curanet's control activity	Tests performed by PwC	Result of PwC's tests
8.32	*Change management* *Planned changes* Planned changes are documented according to a standardised process that ensures that maintenance announcements are made with the required information. All maintenance announcements are processed and approved by the CTO.	Inquired about the process for changes and verified that the process is system-supported to ensure that required information for maintenance announcements is specified. For selected samples, Inspected that all required information is included in the maintenance announcement and that it is processed and approved by the CTO.	No exceptions noted.

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."

Lotte Bendstrup

MD

På vegne af: Curanet A/S

Serienummer: lotte.bendstrup@team.blue

IP: 185.25.xxx.xxx

2025-03-05 14:58:10 UTC

Lotte Bendstrup

Rico Lundager

PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231

Senior manager

På vegne af: PricewaterhouseCoopers Statsautoriseret…

Serienummer: 2e75390a-f48a-4123-b26c-3fd3e97823aa

IP: 83.136.xxx.xxx

2025-03-05 15:13:55 UTC

Jesper Parsberg Madsen

PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231

Statsautoriseret revisor

På vegne af: PricewaterhouseCoopers Statsautoriseret…

Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e

IP: 87.49.xxx.xxx

2025-03-05 15:17:19 UTC

Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptofrafiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl med brug af certifikat og tidsstempel fra en kvalificeret tillidstjenesteudbyder.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskriveres digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, **https://penneo.com/validator**, eller andre valideringstjenester for digitale underskrifter