www.pwc.dk

# *Netic A/S*

## Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2021 to 31 December 2021 in relation to Netic A/S' hosting and operating services

*March 2022*

# Contents

# 1. Management's statement

The accompanying description has been prepared for customers who have used Netic A/S' (Netic) hosting and operating 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 the customers, financial statements.

Netic uses the following as subservice suppliers for hosting services:

- Microsoft Ireland Operations Ltd.
- Amazon Web Services EMEA SARL, Luxembourg
- Google Ireland Limited, Ireland.

This report uses the carve-out method and does not comprise controls that the subservice suppliers perform for Netic.

Netic confirms that:

a) The accompanying description in section 2 fairly presents Netic's hosting and operating services that have processed customers' transactions throughout the period from 1 January 2021 to 31 December 2021. The criteria used in making this statement were that the accompanying description:

(i) Presents how IT general controls in relation to Netic's hosting and operating 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 Netic's hosting and operating 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 the IT general controls

(ii) Includes relevant details of changes to IT general controls in relation to Netic's hosting and operating services during the period from 1 January 2021 to 31 December 2021

(iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to Netic's hosting and operating 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 the IT general controls in relation to Netic's hosting and operating 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 2021 to 31 December 2021. 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 2021 to 31 December 2021.

Aalborg, 25 March 2022
Netic A/S

Steen Jensen
CEO

# 2. Netic's description of IT general controls in relation to hosting and operating services in Denmark

## 2.1. Introduction – briefly about Netic A/S

Netic's primary business areas are hosting, operation/outsourcing, security, consultancy services and technical software development. Netic's customers range from small companies to large organisations; Netic serves as a direct contact for customers, as a partner or as a sub-supplier.

Netic employs approximately 138 people, and Trifork A/S is the majority shareholder of Netic A/S.

## 2.2. Description of services covered by the report

Netic A/S, among other things, provides consultancy services to customers within a wide range of industries. The services may be provided on a stand-alone or ad-hoc basis, under a pre-paid support or framework agreement, or may take the form of full operation and hosting where Netic bears full responsibility.

As Netic has core competencies in a wide range of subject areas, offers many different products and has a high degree of agility. The company is able to resolve large-scale issues at very short notice.

Netic also provides hosting of servers at many different levels, ranging from a single server hosted in our data centre, to which we merely provide power, cooling and internet access, to larger farms of virtual/physical servers, operating high-end solutions in full two-centre operation with redundant databases as backends.

Netic also provides customised solutions, designed to meet the needs of each individual customer, on the basis of core competencies and agility. Netic also has a small portfolio of proprietary solutions.

As standard products/services, Netic offers e.g. virtual servers, Kubernetes solutions, infrastructure, hosting of mail, web, applications and databases on self-operated platforms.

Netic has three physically separated data centres. The data centres are located at different addresses and are secured by use of electronic access control on two mutually independent systems; one of these systems is 100% controlled by Netic A/S.

In all data centres, video surveillance, alarms, fire protection and emergency power equipment (in the form of UPS and generators) have been established. All supply is redundant.

All infrastructure components as well as all general services and customer-specific solutions are subject to automatic monitoring 24-7. To ensure quick response times outside of normal working hours, contingency measures and a service desk have been established.

Netic uses sub-suppliers if our customers request it. Only recognised and well-reputed providers are used. The following hosting sub-suppliers are used:

- Microsoft Ireland Operations Ltd.
- Amazon Web Services EMEA SARL, Luxembourg
- Google Ireland Limited, Ireland.

The description comprises the above items for the period 1 January 2021 to 31 December 2021 and is intended only for companies using Netic's hosting, security and operating services as well as their auditors and may not be used for any other purpose.

## 2.3. Significant changes

During the period from 1 January 2021 to 31 December 2021, no significant changes have been made to Netic's operations that may affect the security and operational stability of our customers.

## 2.4. Control environment

The description of Netic's control environment is divided into the following topics:

### Information security policies

Netic endeavours to ensure that relevant controls are based on the ISO 27001 standard, and they are described in Netic's IT security policy.

### Organisation of information security

The management team responsible for the day-to-day operation of Netic consists of Steen Jensen, CEO, John Zimmer, COO, Claus Hansen, CCO, Henrik Skovfoged, TS Business Unit Lead, and Karsten Thygesen, CTO.

Netic has established functional responsibility for the described services as well as segregation of duties in relation to critical systems.

Excerpt from Netic's security policy:

*"The operational responsibility for the day-to-day management of information security rests with Netic's CISO (Chief Information Security Officer), see Appendix 1. The CISO ensures that activities, standards, guidelines, controls and measures described in the security manual are implemented and observed. Furthermore, it is important that information security is integrated into all business procedures, operational tasks and projects."*

### Employee security

Any change to Netic's IT security policy or IT security manual will be distributed to all employees. New employees are required to read policies and manuals prior to reviewing these together with Netic's CISO in order to get answers to their questions and to establish their security awareness at an appropriate level. Netic requires all employees at Netic to have a clean criminal record.

### Access management

Netic's general policy on access to systems is that access is only allowed if it serves a legitimate purpose. This applies to physical as well as logical access. Where technically feasible, all access to systems must be logged with accurate information on time and identification of the user who accessed the system in question. Those of Netic's employees being part of the 24/7 duty system have access to all operations-critical systems as this is required to maintain a 24/7 contingency preparedness. All other access is granted only when there is an essential and imperative need. Customers only have access to their own systems. For systems that contain sensitive personal data, they often only have access to a limited part of the system so that data security is maintained, and access is limited as much as possible. Some systems require segregation of duties, and other conditions for access may consequently exist. These conditions are documented for the individual systems.

### Managing assets and systems

New assets are registered in Netic's fixed assets register and/or CMDB depending on the nature of the asset. All assets are kept in good security condition through support agreements, upgrade of software and firmware to secure versions, ongoing patch management according to the customer contract and Netic's patch management policy, etc.

Netic has a policy on the destruction of data dictating that when abolishing assets, storage media will be destroyed on location and will not be returned with data to a manufacturer for service, upgrading or the like.

## Cryptography

All data connections transmitting confidential, personal or sensitive data must be strongly encrypted with up-to-date technology.

Data extracts containing sensitive data transmitted between Netic and Netic's customers and/or business partners must be encrypted, only allowing the intended party to open them. For this purpose, Netic recommends the use of PGP. Data extracts include all types of sensitive data on all types of media – for example CDs, USB sticks, emails and digital uploads.

## Physical and environmental security

Customer data is stored on IT systems in Netic's data centres. These data centres are protected by electronic access control with two-factor access, electronic burglary monitoring by a security firm, video surveillance and several layers of physical security. Internally in the data centres, customers, who themselves have access, are physically separated, and certain critical systems are moreover physically separated from the ordinary operational systems.

## Operations security

Where technically feasible and financially reasonable, the design of all IT systems, e.g. networks, servers, IT systems and the like, is based on the principle of no single point of failure.

All data centres are physically placed in buildings with a high security level and several layers of physical security. The data centres are protected against operational loss incidents through the use of aspiration systems and Inergen-based fire suppression, battery/UPS backup, generator-based emergency power and redundant power supply for equipment.

Redundant internet connections from several ISPs always exist – all of them in cables carried in different routings – inside as well as outside the buildings. Furthermore, the data centres are connected internally by several fibre cables carried by different routings and with different routings in the buildings.

All critical data centre components are monitored 24/7 by an on-call duty system.

Netic has prepared and maintains contingency plans describing principles for decision-making power, organisation, communication and remediation of unexpected emergency situations. Furthermore, the contingency plans contain descriptions of a number of options in case of different well-reasoned scenarios to be able to get back to normal operations as quickly as possible. The contingency plans cover physical problems such as fire, water, theft, vandalism, power outage etc. as well as logical problems such as data loss, logical breakdowns, hacking and data theft. The contingency plans are maintained on an ongoing basis and are tested through contingency exercises.

## Acquisition, development and maintenance of systems

The development, operation and maintenance of systems are always based on the security requirements for the processing of data to ensure that data is protected during processing, transportation and storage. Systems are maintained through high-frequency automated patch management with the option of extra patching in emergency situations. Routine vulnerability scans are conducted, and employees are continuously informed and updated on security requirements and procedures applicable when working on systems with sensitive data.

## Supplier relationships

All suppliers of Netic must comply with Netic's IT security policy and must be instructed in Netic's IT security manual to the extent necessary. If a supplier needs access – whether physical or logical – to systems containing customer data, the supplier will be closely accompanied by a Netic employee.

## Information security incident management

As described in Netic's IT security policy:

*"If an employee detects threats to information security or breaches of it, this must immediately result in the creation of an Incident in Netic's incident reporting system and be reported to Netic's CISO."*

### Information security aspects of business continuity management

In emergency or recovery situations, Netic's IT security policy is still applicable and cannot be set aside at any time.

### Minimum requirements for good hosting

Netic aspires to always follow best practice for hosting and maintain a high level of ethics and credibility.

## 2.5. Customers' responsibilities

As part of the delivery of services, the customers must implement certain controls that are important to achieve the control objectives specified in the description. This includes:

- If not explicitly specified in the contract, customers are required to inform Netic whether they want antivirus software to be installed. Customers who have chosen not to have antivirus on their servers are informed that antivirus, and the possible consequences of not having antivirus installed, is on their own responsibility.

- Setting up and administering own users of the solution in the production environment (identity and access management).

- Setting up and administering users from Netic who have access to the customer's environment (identity and access management).

# 3. 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 2021 to 31 December 2021 in relation to Netic A/S' hosting and operating services**

To: Netic, Netic's customers and customers' auditors

### Scope

We have been engaged to provide assurance about Netic's description in section 2 of its IT general controls in relation to Netic's hosting and operating services which have processed customers' transactions throughout the period from 1 January 2021 to 31 December 2021 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Netic uses the following as subservice suppliers for hosting services:

- Microsoft Ireland Operations Ltd.
- Amazon Web Services EMEA SARL, Luxembourg
- Google Ireland Limited, Ireland.

This report uses the carve-out method and does not comprise controls that the subservice suppliers perform for Netic.

### Netic's responsibilities

Netic is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives 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.

PricewaterhouseCoopers is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

### Service auditor's responsibilities

Our responsibility is to express an opinion on Netic's description and on the design and operating effectiveness 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 plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its hosting and operating service 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 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 and described by Netic in the Management's statement section.

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

### Limitations of controls at a service organisation

Netic'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 its hosting and operating services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any 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 outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to Netic's hosting and operating services were designed and implemented throughout the period from 1 January 2021 to 31 December 2021;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2021 to 31 December 2021; 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 January 2021 to 31 December 2021.

### 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

This report and the description of tests of controls in section 4 are intended only for customers who have used Netic's hosting and operating services and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Aarhus, 25 March 2022
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Rico Lundager
Senior Manager

# 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 functionality 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.<br>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 2021 to 31 December 2021. 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 have included how the controls are performed. |
| *Observation* | We have observed the execution of the control. |
| *Reperformance of the control* | Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed. |

## 4.3. Control objectives, control activity, tests and test results

**Control objective A:** ***Information security policy***

*Management has prepared a security policy which outlines clear IT security objectives, including choice of framework and resource allocation. The information security policy is maintained with due consideration of an up-to-date risk assessment.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| A.1 | *Written information security policy*<br>The information security policy has been documented and maintained through review at least once a year. The policy has been approved by Management.<br>The information security policy has been made available to employees via docs.netic.dk. | We have made inquiries of Management about the procedures/control activities carried out.<br>By inspection, we have checked that Management has approved the security policy and that the policy is subject to review at least once a year. We have furthermore checked that employees have easy access to the policy. | No exceptions noted. |

**Control objective B: *Organisation of information security***

*The organisational responsibility for information security is documented and implemented, and security is given high priority in agreements with external parties.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| B.1 | *Management's information security-related responsibility*<br>The organisational responsibility for information security is documented and implemented. Furthermore, rules on communication with customers and reporting on information security incidents have been laid down. | We have made inquiries of Management about the procedures/control activities carried out.<br>By inspection, we have checked that the organisational responsibility for information security has been documented and implemented.<br>We have observed communication with clients regarding information security incidents. | No exceptions noted. |
| B.2 | *Records of assets*<br>Records of physical and logical assets have been prepared. Logical assets are maintained dynamically in Netic's systems. | We have made inquiries of Management about the procedures/control activities implemented.<br>We have verified that records of logical assets have been prepared. | No exceptions noted. |
| B.3 | *External parties*<br>Risks related to external parties are identified, and security in third-party agreements as well as security issues related to customers are addressed.<br>Services delivered by service providers have been reviewed, and due consideration has been given to whether or not auditor's reports should be obtained from these, e.g. a 3402 report. New reports are reviewed at regular intervals to ensure that they cover the correct period. Identified control weaknesses are moreover reviewed. | We have made inquiries of Management about the procedures/control activities implemented.<br>We have observed that audit reports have been received from the relevant service organisations for the relevant period. | No exceptions noted. |

**Control objective C: *Physical security***

*Operations are conducted out of premises protected from damage resulting from physical factors such as fire, water leaks, power outage, theft or vandalism.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.1 | *Physical security perimeter*<br>Access to secure areas (for both new and existing employees) is limited by use of access cards to authorised employees and requires documented Management approval.<br>Individuals without clearance to access secure areas must be registered and accompanied by an employee with the appropriate authorisation.<br>At regular intervals, Netic collects and reviews access lists from NOVI Service and ensures that only individuals with a work-related need have access to the data centres. | We have made inquiries of Management about the procedures/control activities carried out. During visits to the data centres, we observed that access to secure areas is limited by use of an electronic access control system.<br>Using random samples, we have reviewed procedures for physical security in secure areas to assess whether access to these areas is subject to documented Management approval and whether individuals without authorisation are registered and accompanied by an employee with proper authorisation.<br>Using random samples, we have moreover reviewed employees with access to secure areas and verified that documented Management approval has been granted. | No exceptions noted. |
| C.2 | *Securing of offices, premises and facilities*<br>For all server rooms, an access control system has been installed, and physical locks have been applied; these ensure that access is restricted to employees with the appropriate authorisation.<br>Review of existing access rights is carried out every six months. | We have made inquiries of Management about the procedures performed.<br>We have inspected all server rooms and verified that access routes have been secured by use of a card reader.<br>By inspection, we have furthermore checked that the procedure for periodic review of the list of authorised employees has been followed. | No exceptions noted. |

**Control objective C: *Physical security***

*Operations are conducted out of premises protected from damage resulting from physical factors such as fire, water leaks, power outage, theft or vandalism.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| C.3 | *Location and protection of equipment*<br>Data centres are protected against physical threats such as fire, water and heat. Moreover, equipment has been installed to monitor the indoor climate, including humidity and temperature. These parameters are monitored by Netic's monitoring system. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have verified that fire-fighting equipment and cooling have been installed in the data centres.<br>We have furthermore verified that equipment has been installed to monitor the indoor climate in the data centres.<br>Using random samples, we have reviewed documentation of equipment maintenance to confirm that such maintenance is performed on an ongoing basis. | No exceptions noted. |
| C.4 | *Supporting utilities (security of supply)*<br>Data centres are protected from power failure by the use of UPS (uninterruptible power supply) and emergency power facilities. Separate emergency power facilities have been installed for each data centre.<br>Data centres have been fitted with independent and redundant fibre connections that ensure a stable Internet connection. | We have made inquiries of Management about the procedures/control activities carried out.<br>During our visits to the data centres, we observed that monitoring of UPS or emergency power facilities takes place.<br>Using random samples, we have reviewed documentation of equipment maintenance to confirm that UPS or emergency power facilities are subject to regular maintenance and test activities.<br>We have verified that independent and redundant fibre connections to data centres have been established. | No exceptions noted. |
| C.5 | *Securing of wiring* | We have observed that cables for the supply of electricity and data communication are protected against damage and unauthorised actions. | No exceptions noted. |

**Control objective D:** ***Communications and operations management***

*The below measures have been established:*

- *Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents*
- *Sufficient procedures for backup and contingency plans*
- *Appropriate segregation of duties in and around IT functions, including between development, operations and user functions.*
- *Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| D.1 | *Documented operating procedures*<br>Operating procedures are documented on docs.netic.dk.<br>Baselines and template descriptions for virtual machines and databases are in place.<br>Procedures and process descriptions for changes, incidents, service requests and monitoring of standard operations have been established. | We have made inquiries of Management about whether all relevant operating procedures have been documented.<br>In connection with the audit of each area of operation, we have checked that documented procedures are in place and that there is consistency between documentation and actions performed. | No exceptions noted. |
| D.2 | *Segregation of duties*<br>Management has implemented policies and procedures to ensure satisfactory segregation of duties.<br>These policies and procedures include the following requirements:<br>• Development and operating activities are to be completely separated where this is relevant to standard operating services.<br>• Segregation of duties is to be applied to backup and log functions.<br>Development activities are not included in Netic's standard operating services. | We have made inquiries of Management about the procedures/control activities carried out.<br>By inspection, we have checked that users with administrative access rights have a work-related need for such rights and that access rights do not compromise segregation of duties in relation to the development and production environments.<br>Furthermore, we have checked that the number of users with logical access to backup and log functions is limited in order to confirm that segregation of duties is upheld for the functions in question. | During our audit of privileged access, we were informed that privileged access is granted through membership of a group. We were informed that a centralised list of systems to which the groups provide access is not maintained.<br>No further exceptions noted. |

**Control objective D: *Communications and operations management***

*The below measures have been established:*

- *Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents*
- *Sufficient procedures for backup and contingency plans*
- *Appropriate segregation of duties in and around IT functions, including between development, operations and user functions.*
- *Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| D.3 | *Measures to protect against viruses and similar malicious code*<br>Antivirus programmes are installed and updated on employee PCs. | We have made inquiries of Management about the procedures/control activities carried out.<br>Using random samples, we have reviewed employee PCs to confirm that antivirus programs have been installed on relevant platforms and that these are updated. | No exceptions noted. |
| D.4 | *Backup of information*<br>Netic has adopted a backup strategy stating that backup is to take place pursuant to a published backup policy.<br>Every day, an email is sent to the person responsible for backup who follows up on any errors.<br>Backup information for customers and employees and backup overviews are automatically documented.<br>Restore testing is performed every month. Rotation is carried out between employees and subsystems for testing. | We have made inquiries of Management about the procedures/control activities carried out.<br>Using random samples, we have reviewed backup procedures to confirm that these have been formally documented.<br>Using random samples, we have reviewed backup logs to confirm that backup has been successfully completed; alternatively that remedial measures have been taken in case of backup failure.<br>Using random samples, we have reviewed restore logs.<br>We have reviewed the physical security (e.g. restricted access) at off-site storage locations to confirm that backup data are stored in an appropriate manner. | No exceptions noted. |

**Control objective D: *Communications and operations management***

*The below measures have been established:*

- *Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents*
- *Sufficient procedures for backup and contingency plans*
- *Appropriate segregation of duties in and around IT functions, including between development, operations and user functions.*
- *Appropriate business processes and controls pertaining to data communication which seek to prevent loss of authenticity, integrity, availability and confidentiality.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| D.5 | *Monitoring of system use and audit logging*<br>Transactions or activities, as well as users with privileged rights (e.g. super users), are subject to monitoring. This also includes databases. Issues are examined and resolved in a timely manner.<br>All of the above information is stored in a log system. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have verified that log information exists documenting that transactions and activities are stored in the log system and that such information is only made available to individuals with a work-related need. | No exceptions noted. |
| D.6 | *Administrator and operator log*<br>High-risk operating systems and network transactions or activity as well as users with privileged rights are subject to monitoring. Issues are examined and resolved in a timely manner. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have reviewed the system set-up on servers and important network units and verified that the parameters for logging are configured in such a way that actions performed by users with extended rights are logged. | No exceptions noted. |
| D.7 | *Error logging*<br>For all units, a monitoring document exists, specifying what risks and errors are being monitored.<br>The monitoring system generates alerts that are received and assessed by the service desk/person on duty. If relevant, a ticket is created in the case management system. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have verified that the monitoring system is configured to detect and handle errors in automatic transaction processes and that error reports from the system are investigated and managed in due time. | No exceptions noted. |

**Control objective E:** ***Access management***

*The below measures have been established:*

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data as well as logical and physical access controls which reduce the risk of unauthorised access to systems and data.*
- *Logical access controls supporting organisational segregation of duties.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| E.1 | *User registration and privilege administration*<br>All access to operating systems, network, databases and data files for new and existing employees is reviewed to ensure compliance with company policies. Moreover, it is ensured that rights are granted on the basis of a work-related need, approved and created correctly in the systems.<br>At the time of employment, all employees must provide a clean criminal record. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have obtained an overview of the company's and the customers' user accounts on systems and networks. We have randomly selected new users and verified that access right requests for these users have been documented and approved in accordance with the relevant security policy.<br>We have inspected that new employees have provided a clean criminal record. | No exceptions noted. |
| E.2 | *Administration of user access codes (passwords)*<br>Access to operating systems, networks, databases and data files is protected by use of passwords. Requirements have been established for the quality of passwords, i.e. minimum length, complexity and expiry, and password settings ensure that passwords cannot be reused.<br>All shared passwords are stored encrypted in a password manager with differentiated access.<br>All of the company's workstations are secured by use of encryption of hard disks, as specified in the internal IT security manual. | We have made inquiries of Management about procedures/control activities carried out in connection with password controls, and we have verified that users are subject to appropriate authentication on all access points.<br>By inspection, we have checked that appropriate requirements for password quality have been established in Netic's operating environment – by performing random sample tests of whether access to the company's systems is granted on the basis of username and password. | During our audit, we observed that selected customer servers do not comply with Netic's internal password policy.<br>During our audit of selected customer servers, we observed that the lockout policy does not follow a baseline.<br>No further exceptions noted. |

**Control objective E: *Access management***

*The below measures have been established:*

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data as well as logical and physical access controls which reduce the risk of unauthorised access to systems and data.*
- *Logical access controls supporting organisational segregation of duties.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| E.3 | *Assessment of user access rights*<br>Management periodically reviews user access rights to ensure alignment with the users' work-related needs. Discrepancies are investigated and resolved in a timely manner. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have randomly checked that periodic reviews have been performed.<br>We have randomly verified that identified deviations are subject to remedial action. | During our audit, we observed that an assessment of privileged accounts has been performed within the period. We have been informed that the design of the control does not include a formal update of access before it is approved.<br>No further exceptions noted. |
| E.4 | *Revoking access rights*<br>User rights granting access to operating systems, networks, databases and data files pertaining to employees who have left the company are revoked in a timely manner. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have obtained an overview of revoked access rights for the company's and the customers' user accounts. Using random samples, we have compared this overview with the list of current user accounts and verified that the user accounts have been deleted or assigned to a new user. For user accounts that have not been deleted or assigned to a new user in accordance with the determined security policy, we have verified that documentation is in place of network and physical access having been revoked. | No exceptions noted. |

**Control objective E:** ***Access management***

*The below measures have been established:*

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data as well as logical and physical access controls which reduce the risk of unauthorised access to systems and data.*
- *Logical access controls supporting organisational segregation of duties.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| E.5 | *Policy on use of network services, including authentication of users with external connections*<br>Data communication is conducted in accordance with appropriate processes and controls which seek to reduce the risk of loss of authenticity, integrity, availability and confidentiality. Where necessary, Netic has effected segregation of networks, pursuant to agreement with its customers. The office network is segmented in relation to employee groups based on certificates. | We have made inquiries of Management about the procedures/control activities carried out.<br>By inspection, we have checked that users are identified and verified prior to access rights being granted and that remote access is protected by use of VPN.<br>We have inspected the firewall configuration and checked that Netic makes use of intrusion detection systems built into firewalls and load balancer; security precautions that actively and continually provide information on changes that may affect the confidentiality, integrity and availability of data.<br>By inspection, we have checked that networks have been set up with DMZ zones. | During our audit, we observed that filters have been set up that only allow access to customer networks for employees with a work-related need. However, a legacy network still exists that allows access to customer networks for all employees. We have been informed that the legacy network was closed on 14 June 2021.<br>No further exceptions noted. |
| E.6 | *Management of network connections*<br>Vulnerability scans are conducted at regular intervals to ensure network security.<br>Firewall logs and load balancers are stored in Splunk to enable traceability. | We have made inquiries of Management about the procedures/control activities carried out.<br>By observation, we have checked that vulnerability scans are carried out at regular intervals.<br>We have observed that identified weaknesses have been assessed and remedial action has been taken. | No exceptions noted. |
| E.7 | *Procedures for secure log-on*<br>Access to operating systems and networks is password-protected through centralised LDAP and Kerberos, where possible.<br>Requirements have been established for the quality of passwords, i.e. minimum length, complexity and expiry. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have inspected extracts from LDAP and Kerberos and reviewed password quality requirements. | No exceptions noted. |

**Control objective E:** ***Access management***

*The below measures have been established:*

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data as well as logical and physical access controls which reduce the risk of unauthorised access to systems and data.*
- *Logical access controls supporting organisational segregation of duties.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| E.8 | *Limited access to information*<br>All access requests for new and existing users concerning applications, databases and data files are reviewed via the service request in JIRA to ensure compliance with the company's policies; this to ensure that rights are granted on the basis of a work-related need, are approved and created correctly in systems. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have verified that access requests for new and existing users are managed in JIRA. | No exceptions noted. |

**Control objective F:** ***Acquisition, development and maintenance of operating systems***

*Appropriate procedures and controls have been established for implementation and maintenance of operating systems.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| F.1 | *Management of software in operating systems*<br>Netic has the operational responsibility for security patching the servers, network equipment and a number of other applications. Netic ensures that the components and applications are patched according to best practice.<br>Patching is done, unless otherwise agreed, during night-time.<br>Patching takes place at least on a monthly basis but can be scheduled more often if this is stated in the contract. | We have made inquiries of Management about the procedures/control activities carried out, including about procedures for patching.<br>We have inspected a number of randomly selected servers to verify current patch level is in accordance with patch policy. | No exceptions noted. |
| F.2 | *Change management*<br>Changes to parts of production and networks are tested/simulated and approved by qualified personnel prior to being moved to production.<br>Netic has a complete and documented procedure for the implementation of changes. This is carried out via Netic's JIRA, in which a pre-determined workflow is executed.<br>All changes are normally approved by an ITIL-trained change manager prior to implementation. | We have made inquiries of Management about the procedures/control activities carried out.<br>Using random samples, we have reviewed change requests for the following:<br>• Documented test of changes, including approval.<br>• Approval must be obtained prior to implementation. Oral Management approval is considered sufficient in connection with emergency changes; subsequently, such approval must be documented.<br>Documented plan for roll-back, where relevant. | No exceptions noted. |

**Control objective G: *Disaster recovery plan***

*Netic is able to continue its service delivery to its customers in case of a disaster situation.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| G.1 | *Set-up/structure of Netic's disaster recovery*<br>The entire disaster recovery plan is comprised of a high-level disaster recovery procedure and operational disaster recovery plans for the specific disaster areas.<br>The operational disaster recovery plan includes a description of the disaster organisation, i.e. descriptions of Management functions, contact information, notification lists and instructions for the requisite disaster task forces.<br>For the individual platforms, detailed task force instructions have been prepared concerning recovery and emergency operation. | We have made inquiries of Management about the procedures/control activities carried out.<br>We have reviewed the materials provided on disaster preparedness, and we have verified that the organisational and operational IT disaster recovery plan includes Management function descriptions, contact information, notification lists as well as instructions. | No exceptions noted. |

**Control objective H: *Disaster recovery test***

*Netic is able to continue its service delivery to its customers in case of a disaster situation.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| H.1 | *Test of Netic's disaster recovery*<br>Annually, a test is performed of disaster recovery comprising desktop tests and realistic test scenarios. | Using random samples, we have checked that contingency plans are tested through desktop tests or realistic test scenarios to the extent possible. | No exceptions noted. |

# 5. Additional information from Netic

The information included in this section is prepared by Netic to provide the customer with further information. The section should not be regarded as a part of the system description. The information in this section is not covered by audit procedures performed to assess whether the system description gives a true and fair view, whether the controls supporting the control objectives presented in section 4 have been suitably designed and whether they operated effectively throughout the period. Thus, PwC's conclusion in section 3 does not cover the information in section 5.

Under the control activity D.2 *"Segregation of duties",* PwC states:

"During our audit of privileged access, we were informed that privileged access is granted through membership of a group. We were informed that a centralised list of systems to which the groups provide access is not maintained".

For this observation, Netic states that the description of systems managed by the privileged group is limited to IDP systems, backup systems and password management systems. A more detailed description will be written and included during the ISO 27001 process.

Under the control activity E.2*"Administration of user access codes (passwords)",* PwC states:

"During our audit, we observed that selected customer servers do not comply with Netic's internal password policy. During our audit of selected customer servers, we observed that the lockout policy does not follow a baseline.

For this observation, Netic states that during 2021 all root accounts were set with individual passwords with special password requirements that differ a bit from standard requirements for practical reasons. Securing the root account is a major step in improving security as the local user is only used on a limited number of servers. Action for rolling out the required software for enforcing specific local user password rules is still ongoing. The lockout policy is "After five failed logon attempts, the security incident is handled by Netic SOC. The SOC is manned 24/7/365. The process is not fully implemented for all servers.

Under the control activity E.3 *"Assessment of user rights",* PwC states:

"During our audit, we observed that an assessment of privileged accounts has been performed within the period. We have been informed that the design of the control does not include a formal update of access before it is approved".

For this observation, Netic will update the design and process in 2022.

Under the control activity E.5 *"Policy on use of network services, including authentication of users with external connection",* PwC states:

"During our audit, we observed that filters have been set up that only allow access to customer networks for employees with a work-related need. However, a legacy network still exists that allows access to customer networks for all employees. We have been informed that the legacy network was closed on 14 June 2021".

For this observation, Netic informed PwC that the legacy network was closed on 14 June 2021.

PENNEO

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

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

**Steen Jensen**
**Kunde**
På vegne af: Netic A/S
*Serienummer: PID:9208-2002-2-013933737584*
*IP: 77.243.xxx.xxx*
*2022-03-25 10:15:19 UTC*
NEM ID ✓

**Rico Lundager**
**Revisor**
På vegne af: PricewaterhouseCoopers Statsautoriseret...
*Serienummer: CVR:33771231-RID:30016557*
*IP: 208.127.xxx.xxx*
*2022-03-25 10:18:50 UTC*
NEM ID ✓

**Jesper Parsberg Madsen**
**Statsautoriseret revisor**
På vegne af: PricewaterhouseCoopers Statsautoriseret...
*Serienummer: PID:9208-2002-2-427963640472*
*IP: 80.62.xxx.xxx*
*2022-03-25 10:30:54 UTC*
NEM ID ✓

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

**Sådan kan du sikre, at dokumentet er originalt**
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validate**