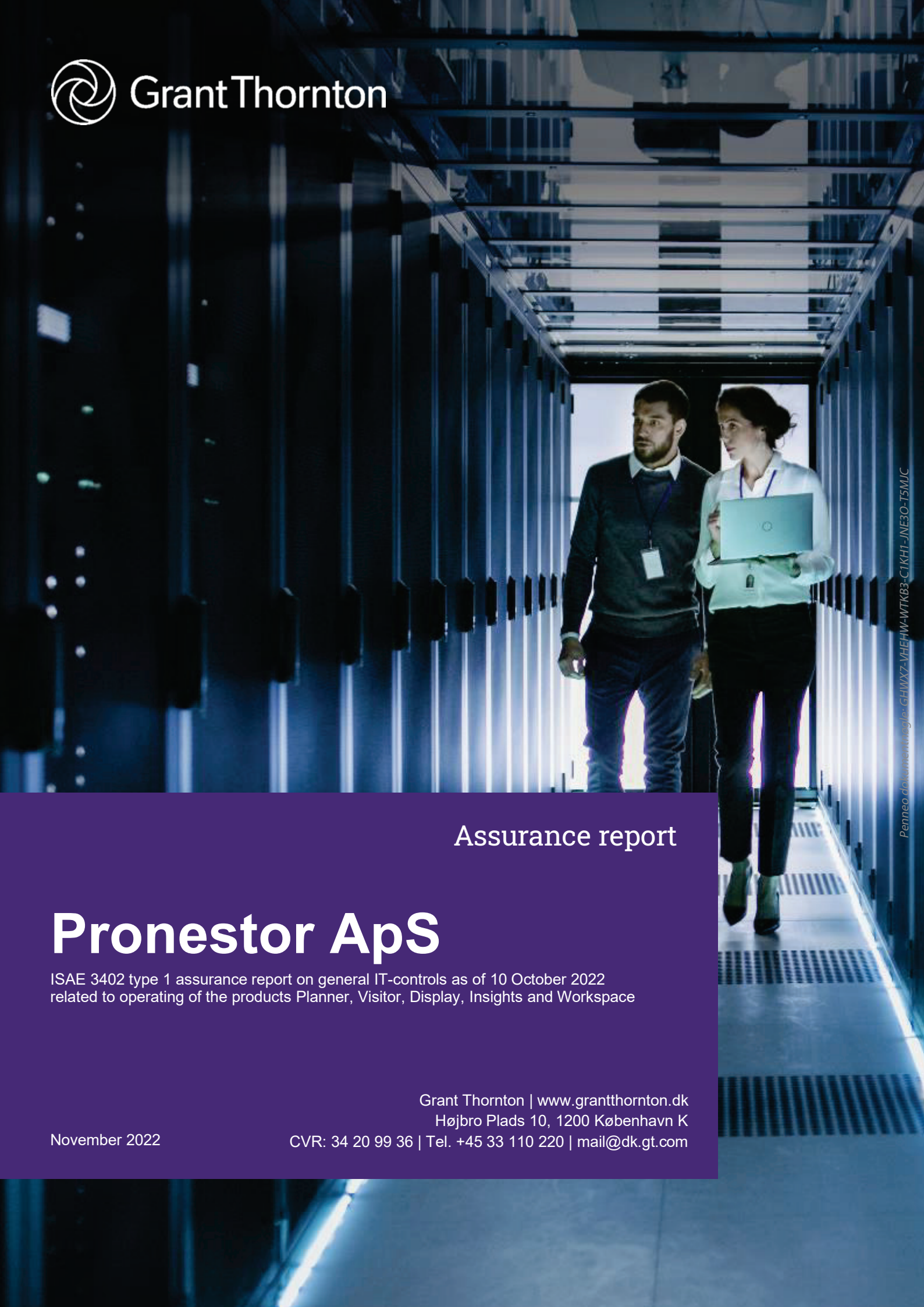

Assurance report

# Pronestor ApS

ISAE 3402 type 1 assurance report on general IT-controls as of 10 October 2022
related to operating of the products Planner, Visitor, Display, Insights and Workspace

November 2022

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tel. +45 33 110 220 | mail@dk.gt.com

Table of contents

# Section 1: Description of Pronestor ApS' services in connection with operating of the products Planner, Visitor, Display, Insights and Workspace, and related general IT-controls

Pronestor offers these five cloud-based products as a hosted and managed solution for our customers.

- Planner
- Visitor
- Display
- Insights
- Workspace

This declaration encompasses the general processes and system setup necessary for hosting and managing these systems. Processes and system setup for custom individual agreements with any of Pronestor's customers are not covered by this declaration.

## General IT-controls at Pronestor

### Introduction

The services listed in paragraph 1.1 are a number of applications characterized by being standard software, which means that all Pronestor customers subscribing to a solution has access to the same solution and the same versions of the solution in question.

This means that the security measures and controls described in this document as well as all other policies, risk evaluations, procedures and controls cover all cloud-based products for all customers.

### Use of subservice organisations

Pronestor uses subsuppliers for the following services.

- SMS notifications
- E-mail notifications
- Cloud hosting
- Source Code version control
- Vulnerability and penetration testing
- ITSM-systems

### Risk assessment and management

Pronestor has used a standard risk assessment tool to assess the potential impacts of all areas of business. The impact assessment model addresses at minimum the following

- Economic impact
- Data protection (GDPR)
- Data loss
- Availability chain. e.g., reliance on internet connectivity
- Malicious insider

Based on the risk analysis severity and likelihood is scored with the following values.

- High – 3
- Medium – 2
- Low – 1
- Inconsequential – 0

Based on the risk assessment and ISO 27001, Pronestor has chosen the main areas and control objectives for it-security management, as described in the following:

## A. 5 Information security policies

The information security policies in Pronestor are developed and maintained by the Pronestor Security Organisation and as a minimum on an annual basis approved by the management team as well.

The Security Policy is available on the intranet for all employees and new employees will be made aware of the policy as part of the onboarding process.

## A. 6 Organisation of information security

The organisation of it-security is based upon Pronestor's it-security policy and origins from ISO27001/2:2013, which contains the following main areas:

| | | | |
|---|---|---|---|
| 5 | Information security policies | 12 | Operations security |
| 6 | Organisation of information security | 13 | Communications security |
| 7 | Human resource security | 14 | Acquisition, development and maintenance of systems |
| 8 | Asset management | 15 | Supplier relationships |
| 9 | Access control | 16 | Information security incident management |
| 10 | Cryptography | 17 | Information security aspects of business continuity management |
| | | 18 | Compliance |

Management of information security within the individual areas, are described below. Control objectives and controls, chosen by Pronestor, are also stated in the summary in section 4.

The management of Pronestor has defined and allocated all information security responsibilities and established an Information Security Organization.

The Information Security Framework implemented ensures that the responsibilities within the security organization are explicit and visible. Organizational duties are segregated in a way that functions with conflicting interests are distributed on different staff.

## A. 7 Human resource security

Prior to employment, Pronestor ensures that employees understand their responsibilities, and that they are suitable for the roles for which they are considered.

Depending on the role and responsibilities the candidate is to take on, there might be more gates for the candidate to pass before reaching the final phase and to be offered a contract. Finally, all employment contracts include a non-disclosure agreement covering information related to customer data, sales and marketing data, strategy, and other confidential business data.

We ensure that our employees receive continuous security training. This is done by sharing internal knowledge, relevant external courses, and certifications. All new employees must go through an information security onboarding session.

## A. 8 Asset management

To ensure that all assets are handled with the proper attention ownership of assets is explicit. The ownership of all production related assets such as customer data, production environments and development environments fall on the CTO. Internal hardware and internal networks are the responsibility of the Internal Help Desk. Procedures are in place to ensure that inventory of assets are kept up to date and that hardware and mobile devices are disposed of securely to protect the confidentiality of Pronestor's customers.

### Mobile devices and teleworking

A mobile device policy and remote work procedure is in place to minimize the risk of portable workstations and remote work. Encryption and remote control of devices is in place. All staff goes through mandatory training in proper handling of information security when outside the office.

## A. 9 Access control

Pronestor ensures that access to information and information processing facilities is limited. The Access control policy is based on a least privilege principle. Privileged access assignments may be segregated into organizational units such as marketing, development, customer support or sales.

Access control includes enforced MFA (Multi Factor Authentication) and use of encrypted password managers.

User access is reviewed on a regular basis and reviews are recorded. Upon employee role changes or terminations, Pronestor handles off-boarding from central systems.

## A. 10 Cryptography

Pronestor employs encryption both at rest and in transit. Encryption in transit uses at least TLS 1.2. SSL 1.0, SSL 2.0, and SSL 3.0 are always disabled. All secrets such as user passwords used in systems are stored in a one-way hashed form using a salted hashing algorithm. Secrets are never stored in clear text.

## A. 12 Operations security

A policy on operational procedures has been established, and a change management workflow has been implemented to ensure the control of changes to the production environments and infrastructure.

Pronestor's Operations Manual contains information about essential areas of daily operations. Incidents are collected from various tools and sent to an alerting system that alerts relevant people. After an incident, a post-mortem is held.

Capacity monitoring is done on metrics from applications, databases and infrastructure. When thresholds are exceeded, alerts are triggered to allow operations staff to scale, as necessary. Development, testing and operational environments are completely separate from each other. Information saved in databases is backed up continuously and copied to the external storage.

Logs are stored in Pronestor's log aggregation system to allow for correlation across systems and easy trouble shooting.

## A. 13 Communications security

Test, staging and production environments are segmented by separate networks and physically separated from the Pronestor office network. Changes to network infrastructure and firewalls are handled as peer reviewed terraform code changes in Pronestor's version control system Git.

## A. 14 Acquisition, development, and maintenance of systems

Pronestor information systems are designed and implemented according to the system development and security life cycle. The process is structured and ensures a consistent high level of security and quality. Established change management workflow ensure that only relevant and necessary changes are made.

## A. 15 Supplier relationships

A process for assessing and managing risks associated with suppliers exists to protect Pronestor and their customers when using suppliers. Supplier relationships are monitored, reviewed and audited on a regular basis to make sure suppliers adhere to both regulations and Pronestor's IT Security Policies.

## A. 16 Information security incident management

Procedures are in place to ensure a consistent and fast approach to information security incidents. The process describes communication both internally and externally. Regulatory requirements are part of these procedures to ensure that any breaches are not just handled promptly and effectively but are also reported to any relevant authorities. Post-mortems are an integral part of any incident to extract any learnings made during the incident.

## A. 17 Information security aspects of business continuity management

Business continuity is planned for both on a daily operational level and on a management level. Business continuity plans exist to make sure management is effective and in sync and that production environments can be restored quickly.

## A.18 Review of information security

A control measure for the management of information security has been implemented and the implementation (i.e., control objectives, controls, policies, processes and procedures for information security) have been independently reviewed on a regular basis or in case of significant changes. Management review on a regular basis whether the information processing and the procedures within their fields of responsibility comply with relevant security policies, standards and other safety requirements. Information systems are regularly reviewed to ensure compliance with the company's security policies and standards.

## Complementary controls with the customers

The controls are designed in such a way that some of the controls mentioned in this declaration must be complimented by controls on the customer side. The controls mentioned below are expected to be implemented and executed at and by the customer in order for Pronestor to be able to fully comply with the controls in this report. The list of controls below should not be considered complete and exhaustive, and where deemed necessary, the customer should add additional controls.

- Customers themselves are responsible to establishing a connection to the Pronestor servers. This includes the responsibility to have a functioning and adequate internet connection as well as tested and verified backup internet connections in case of connectivity issues.
- Customers themselves are responsible for administration of their own user accounts on application, system, and database level.
- Customers themselves are responsible for a regular audit of their own user accounts on application, system, and database level.
- Customers themselves are responsible for making sure created user accounts on application, system and database level are in sync with their employee rooster.
- Should doubt arise on whether a user account has been compromised by for example laptop theft or similar, it is the responsibility of the customer to inform Pronestor of the concern.
- Customers themselves are responsible for establishing a Continuity Plan to handle the customers company in case of emergency, major accidents, or disaster.

# Section 2: Pronestor ApS' statement

The accompanying description has been prepared for customers who have used Pronestor ApS' products Planner, Visitor, Display, Insights and Workspace and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Pronestor ApS is using subservice organisations Microsoft A/S, Zendesk, Compaya and Amazon Web Services. This assurance report is prepared in accordance with the carve-out method and Pronestor ApS' description does not include control objectives and controls within Microsoft A/S, Zendesk, Compaya and Amazon Web Services.

Some of the control objectives stated in Pronestor ApS' description in Section 1 of general IT-controls, can only be achieved if the complementary controls with the customers have been appropriately designed and works effectively with the controls with Pronestor ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Pronestor ApS confirms that:

(a) The accompanying description in Section 1 fairly presents the general IT-controls related to Pronestor ApS' products Planner, Visitor, Display, Insights and Workspace processing customer transactions as of 10 October 2022

The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The type of services provided
- The procedures within both information technology and manual systems, used to manage general IT-controls
- Relevant control objectives and controls designed to achieve these objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to general IT-controls

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

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and implemented as of 10 October 2022. 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.

Kgs. Lyngby, 1 November 2022
Pronestor ApS

Karsten Johan Busck
CEO

# Section 3: Independent service auditor's assurance report on the description of controls, their design and implementation

To Pronestor ApS, their customers and their auditors.

## Scope

We have been engaged to provide assurance about Pronestor ApS' description in Section 1 of its system for delivery of Pronestor ApS' products Planner, Visitor, Display, Insights and Workspace and the related general IT-controls as of 10 October 2022 (the description) and on the design and implementation of controls related to the control objectives stated in the description.

Pronestor ApS is using subservice organisations Microsoft A/S, Zendesk, Compaya and Amazon Web Services. This assurance report is prepared in accordance with the carve-out method and Pronestor ApS' description does not include control objectives and controls within Microsoft A/S, Zendesk, Compaya and Amazon Web Services.

Some of the control objectives stated in Pronestor ApS' description in Section 1 of general IT-controls, can only be achieved if the complementary controls with the customers (or the specific customer) have been appropriately designed and works effectively with the controls with Pronestor ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

## Pronestor ApS' responsibility

Pronestor ApS is responsible for preparing the description (section 1) and accompanying statement (section 2) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Pronestor ApS is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

## Grant Thornton's independence and quality control

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

Grant Thornton applies International Standard on Quality Control 1[1] and accordingly 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.

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

## Pronestor ApS' responsibility

Our responsibility is to express an opinion on Pronestor ApS' description (Section 1) as well as on the design and implementation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed.

An assurance engagement to report on the description, design and implementation of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and implementation of controls.

The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or implemented. Our procedures included testing the design 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 the service organisation.

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

Pronestor ApS' description in section 1, is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

## Opinion

Our opinion has been formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in Pronestor ApS' statement in Section 2 and based on this, it is our opinion that:

(a) The description of the controls, as they were designed and implemented as of 10 October 2022, is fair in all material respects.
(b) The controls related to the control objectives stated in the description were suitably designed as of 10 October 2022 in all material respects.

## Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section (Section 4) including control objectives, test and test results.

## Intended users and purpose

This assurance report is intended only for customers who have used Pronestor ApS' products Planner, Visitor, Display, Insights and Workspace and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 1 November 2022

**Grant Thornton**
State authorised public accountants

Jacob Helly Juell-Hansen
State authorised public accountant

Basel Rimon Obari
Executive director, CISA, CISM

# Section 4: Control objectives, controls and service auditor testing

## 4.1. Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This statement is issued according to the carve-out method and therefore does not include controls of Pronestor ApS' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Pronestor ApS' customers, are not included in this report.

## 4.2. Tests

We performed our test of controls at Pronestor ApS, by taking the following actions:

| Method | General description |
|---|---|
| Inquiries | Interview with appropriate personnel at Pronestor ApS regarding controls. |
| Observation | Observing how controls are performed. |
| Inspection | Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. |
| Re-performance | Re-performance of controls in order to verify that the control is working as assumed. |

## 4.3. Results of tests

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the general IT-controls with Pronestor ApS.

| A.5 Information security policies | | | |
|---|---|---|---|
| A.5.1 Management direction for information security<br>Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations | | | |
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 5.1.1 | *Policies for information security*<br>A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties. | We have inspected the information security policy.<br>We have inspected documentation for management approval of the information security policy.<br>We have inspected that the information security policy has been communicated and is available to the employees online. | No deviations noted. |
| 5.1.2. | *Review of policies for information security*<br>The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness. | We have inspected that the information security policy is updated, and that the policy is based on a risk assessment.<br>We have inspected that the review of the information security policy is part of the annual wheel. | No deviations noted. |

## A.6 Organisation of information security

### A.6.1 Internal organisation
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.1.1 | *Information security roles and responsibilities*<br>All information security responsibilities are defined and allocated. | We have inspected that the organisation chart shows the security organisation.<br>We have inspected that the information security roles and responsibilities have been defined. | No deviations noted. |
| 6.1.2 | *Segregation of duties*<br>Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets. | We have inspected that the organisation chart shows the segregation of duties in the organisation.<br>We have inspected that the information security roles and responsibilities have been defined. | No deviations noted. |

### A.6.2 Mobile devices and teleworking
Control objective: To ensure the security of teleworking and use of mobile devices

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 6.2.1 | *Mobile device policy*<br>Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices. | We have inspected the policy for the securing of mobile devices.<br>We have inspected, that technical controls for securing of mobile devices have been defined and communicated to the employees. | No deviations noted. |
| 6.2.2 | *Teleworking*<br>Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites. | We have inspected policy to secure teleworking.<br>We have inspected the security measures for protection of remote workspaces. | No deviations noted. |

## A.7 Human ressource security

### A.7.1 Prior to employment
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 7.1.1 | *Screening*<br><br>Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks. | We have inspected the procedure for employment of new employees, and the security measures needed in the process.<br><br>We have inquired into whether there have been any new employees since the control was designed. | We have been informed, that there have not been any new employees after the control was designed, and therefore, we have not been able to test the implementation of the control.<br><br>No deviations noted. |
| 7.1.2 | *Terms and conditions of employment*<br><br>The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security. | We have inspected standard contracts with employees and consultants in order to determine whether these include information security responsibility.<br><br>We have inspected that the checklist for new employees includes introduction to information security.<br><br>We have inspected that the employee handbook states that employees are committed to reading the information security policy. | We have been informed, that there have not been any new employees after the control was designed and therefore, we have not been able to test the implementation of the control.<br><br>No deviations noted. |

| A.7.2 During employment<br>Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 7.2.1 | *Management responsibility*<br>Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation. | We have inspected the procedure concerning establishing requirements for employees and partners.<br>We have inspected that the management has required the employees to read and understand the information security policy. | No deviations noted. |
| 7.2.2 | *Information security awareness education and training*<br>Employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function. | We have inquired about procedures to secure adequate training and education (awareness training).<br>We have inspected documentation for activities developing and maintaining security awareness with employees. | No deviations noted. |

| A.7.3 Termination and change of employment<br>Control objective: To protect the organisation's interests as part of the process of changing or terminating employment | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 7.3.1 | *Termination or change of employment responsibility*<br>Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor and enforced. | We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment.<br>We have inspected the letter of resignation template which states that:<br>• All assets should be returned, and<br>• The employee is still contractually prohibited against unauthorized use or disclosure of any trade secrets after resignation.<br>We have inquired into whether there has been any termination or change of employment after the procedure has been designed. | We have been informed that no employees have been terminated after the control was designed and therefore, we have not been able to test the implementation of the control.<br>No deviations noted. |

## A.8 Asset management

| A.8.1 Responsibility for assets<br>Control objective: To identify organisational assets and define appropriate protection responsibilities | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 8.1.1 | *Inventory of assets*<br>Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained. | We have inspected whether the inventory list of assets include both employee assets and servers. | No deviations noted. |
| 8.1.2 | *Ownership of assets*<br>Assets maintained in the inventory are being owned. | We have inspected record of asset ownership. | No deviations noted. |

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 8.1.3 | *Acceptable use of assets*<br>Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented and implemented. | We have inspected the guidelines for acceptable use of assets includes guidelines for laptops, telephones, BYOD and more. | No deviations noted. |
| 8.1.4 | *Return of assets*<br>All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement. | We have inspected the procedure for securing the return of assets delivered.<br>We have inquired into whether there has been any termination of employment after the procedure has been designed. | We have been informed that no employees have been terminated after the control was designed and therefore, we have not been able to test the implementation of the control.<br>No deviations noted. |

| A.8.2 Classification of information<br>Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation. | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 8.2.1 | *Classification*<br>Information is classified in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification. | We have inspected the policy for classification of information.<br>We have inspected that information has been risk assessed and classified. | No deviations noted. |
| 8.2.3 | *Handling of assets*<br>Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the organisation. | We have inspected that the procedure for handling assets is aligned with how information is classified. | No deviations noted. |

| A.8.3 Media handling<br>Control objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 8.3.1 | *Management of removable media*<br>Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation. | We have inspected the procedure for management of removable media.<br>We have inspected that there is a record of laptops. | No deviations noted. |
| 8.3.2 | *Disposal of media*<br>Media are being disposed of securely when no longer required using formal procedures. | We have inspected the procedure for disposal of media.<br>We have inquired into whether there has been any disposal of media in the past year. | We have been informed that there has not been any disposal of media in the past year and therefore we have not been able to test the implementation of the control.<br>No deviations noted. |

## A.9 Access control

| A.9.1 Business requirements of access control<br>Control objective: To limit access to information and information processing facilities | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 9.1.1 | *Access control policy*<br>An access control policy has been established, documented and reviewed based on business and information security requirements. | We have inspected the policy of managing access control in order to establish whether it is reviewed and updated. | No deviations noted. |
| 9.1.2 | *Access to network and network services*<br>Users are only being provided with access to the network and network services that they have been specifically authorized to use. | We have inspected the procedure for managing access to networks and network services.<br>We have inspected the extract of users in the system, in order to establish that they only have access to approved networks and services, based on work-related requirements. | No deviations noted. |

| A.9.2 User access management<br>Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services. | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 9.2.1 | *User Registration and de-registration*<br>A formal user registration and de-registration process has been implemented to enable assignment of access rights. | We have inspected the procedure for creating and termination of users.<br>We have inquired into whether there has been any user registrations or de-registrations after the procedure has been designed. | We have been informed that there has been no user registrations or de-registrations after the control was designed and therefore, we have not been able to test the implementation of the control.<br>No deviations noted. |
| 9.2.2 | *User access provisioning*<br>A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services | We have inspected that a procedure for user administration has been established.<br>We have inquired into whether there has been any user access provisioning after the procedure has been designed. | We have been informed that there has been no user access provisioning after the control was designed and therefore, we have not been able to test the implementation of the control.<br>No deviations noted. |
| 9.2.3 | *Management of privileged access rights*<br>The allocation and use of privileged access rights have been restricted and controlled. | We have inquired about procedures for granting rights, use and limitation of privileged access rights.<br>We have inspected the extract of privileged users to establish whether the procedure has been followed.<br>We have inspected that only users with a work-related need, has a privileged access.<br>We have inspected that all privileged access rights have been reviewed. | No deviations noted. |
| 9.2.4 | *Management of secret-authentication information of users*<br>The allocation of secret authentication information is controlled through a formal management process. | We have inspected the procedure regarding allocation of passwords to platforms.<br>We have, by sample test, inspected that allocation of passwords follows the procedure. | No deviations noted. |

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 9.2.5 | *Review of user access rights*<br>Asset owners are reviewing user's access rights at regular intervals. | We have inquired into the process of periodic review of users' access rights.<br>We have inspected that there has been a periodic review of users' access rights. | No deviations noted. |
| 9.2.6 | *Removal or adjustment of access rights*<br>Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change. | We have inspected the procedure about discontinuation and adjustment of access rights.<br>We have inquired whether there has been any removal or adjustment of access rights, after the procedure has been designed. | We have been informed that there has been no removal or adjustment of access rights after the control was designed and therefore, we have not been able to test the implementation of the control.<br>No deviations noted. |

| A.9.3 User responsibilities<br>Control objective: To make users accountable for safeguarding their authentication information | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 9.3.1 | *Use of secret authentication information*<br>Users are required to follow the organisations' s practices in the use of secret authentication information. | We have inspected that the password procedure establishes requirements for the use of secret authentification information.<br>We have inspected that two-factor authentication is enforced on all PC's. | No deviations noted. |

| A.9.4 System and application access control<br>Control objective: To prevent unauthorised access to systems and applications | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 9.4.2 | *Secure log-on procedures*<br>Access to systems and applications is controlled by procedure for secure logon. | We have inspected that the procedure for secure log-on requires the use of two-factor authentication and passwords.<br>We have inspected that two-factor authentication is enforced on all PC's. | No deviations noted. |
| 9.4.3 | *Password management system*<br>Password management systems are interactive and have ensured quality passwords. | We have inspected that policies and procedures require quality passwords.<br>We have inquired that systems for administration of access codes are configured in accordance with the requirements. | No deviations noted. |
| 9.4.5 | *Access control to program source code*<br>Access to program source code has been restricted. | We have inspected the procedure for access to program source code.<br>We have inspected that users' access to program source code, are based on a work-related need.<br>We have inspected that access to the program source code is logged. | No deviations noted. |

## A.10 Cryptography

### A.10.1 Cryptographic controls
Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 10.1.1 | *Policy on the use of cryptographic controls*<br><br>A policy for the use of cryptographic controls for protection of information has been developed and implemented. | We have inspected that the cryptography procedure includes requirements for cryptography.<br><br>We have inspected that the requirements for cryptography have been implemented. | No deviations noted. |
| 10.1.2 | *Key Management*<br><br>A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle. | We have inspected the policy for key management.<br><br>We have inquired to the procedure for renewal of the certificates. | No deviations noted. |

## A.12 Operations security

### A.12.1 Operational procedures and responsibilities
Control objective: To ensure correct and secure operation of information processing facilities

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 12.1.1 | *Documented operating procedures*<br>Operating procedures have been documented and made available to all users. | We have inspected the operating procedures.<br>We have inspected that the procedures are available to all users. | No deviations noted. |
| 12.1.2 | *Change management*<br>Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled. | We have inspected that the procedure for change management includes procedures for change to new and existing products.<br>We have, by sample test, inspected that the change management procedures have been followed for implemented changes. | No deviations noted. |
| 12.1.3 | *Capacity management*<br>The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained. | We have inquired into the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements.<br>We have inquired into whether relevant platforms are included in the capacity requirement procedure.<br>We have inspected a sample of capacity management. | No deviations noted. |
| 12.1.4 | *Separation of development-, test- and operations facilities.*<br>Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment. | We have inquired into securing the separation of development-, test- and operations facilities.<br>We have inspected, that development, test and production are either physically or logically separated. | No deviations noted. |

| A 12.2 Protection from malware<br>Control objective: To ensure that information and information processing facilities are protected against malware | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 12.2.1 | *Control against malware*<br>Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness. | We have inquired into measures against malware.<br>We have inspected that anti-virus is enabled on servers. | No deviations noted. |

| A.12.3 Backup<br>Control objective: To protect against loss of data | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 12.3.1 | *Information backup*<br>Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy. | We have inspected the policy for backup.<br>We have inspected the documentation for the setup of backup is in according to the requirements.<br>We have inspected that backup is monitored. | No deviations noted. |

| A.12.4 Logging and monitoring<br>Control objective: To record events and generate evidence | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 12.4.1 | *Event logging*<br>Event logs recording user activities exceptions faults and information security events shall be produced, kept and regularly reviewed. | We have inspected the dashboard for event logs.<br>We have inquired into the procedure for reviewing the logs regularly. | We have been informed, that the logs are reviewed daily, but there is no documentation hereof.<br>No further deviations noted. |
| 12.4.2 | *Protection of log information*<br>Logging facilities and log information are being protected against tampering and unauthorized access. | We have inquired about secure log information, and we have inspected the solution.<br>We have inspected a sample of logging configurations in order to establish whether login information is protected against manipulation and unauthorized access. | No deviations noted. |
| 12.4.3 | *Administrator and operator logs*<br>System administrator and system operator activities have been logged and the logs are protected and regularly reviewed. | We have inquired into procedures regarding logging of activities performed by system administrators and operators.<br>We have inspected logon setups on servers in order to establish whether the actions of system administrators and operators are logged.<br>We have inspected the extract of users with access to administrator and operator logs and inquired whether the access rights are limited to users with a work-related need. | No deviations noted. |
| 12.4.4 | *Clock synchronization*<br>The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source. | We have inspected the procedures for synchronization against a reassuring time server. | No deviations noted. |

| A.12.6 Technical vulnerability management<br>Control objective: To prevent exploitation of technical vulnerabilities | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 12.6.1 | *Management of technical vulnerabilities*<br>Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. | We have inquired into the procedure regarding gathering and evaluation of technical vulnerabilities.<br>We have inspected the vulnerability scan report and inspected the follow-up on the report. | No deviations noted. |

## A.13 Communications security

| A.13.1 Network security management<br>Control objective: To ensure the protection of information in networks and its supporting information processing facilities | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 13.1.1 | *Network controls*<br>Networks are managed and controlled to protect information in systems and applications. | We have inspected the requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and whether other relevant security measures have been defined. | No deviations noted. |
| 13.1.2 | *Security of network services*<br>Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced. | We have inspected that the firewall in the office network is active and updated.<br>We have inspected whether certificates on the domains are active. | No deviations noted. |
| 13.1.3 | *Segregation of networks*<br>Groups of information services users and information systems are segregated on networks. | We have inspected that the network diagram indicates the segregation of networks.<br>We have inspected the list of networks to verify the segregation. | No deviations noted. |

| A.13.2 Information transfer<br>Control objective: To maintain the security of information transferred within an organisation and with any external entity | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 13.2.1 | *Information transfer policies and procedures*<br>Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities. | We have inspected that the IT-security policy includes policies and controls for information transfer.<br>We have inspected that the procedure for cryptography includes procedures for how cloud-services use cryptography.<br>We have inspected that the hardware procedure includes procedures for cryptography on laptops and portable media. | No deviations noted. |
| 13.2.3 | *Electronic messaging*<br>Information involved in electronic messaging is appropriately protected. | We have inquired about guidelines for electronic messaging of confidential information.<br>We have inspected that TLS is used to protect electronic messaging. | No deviations noted. |
| 13.2.4 | *Confidentiality or non-disclosure agreements*<br>Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information, are identified, and documented on a regular basis. | We have inspected the procedure for establishing non-disclosure-agreements.<br>We have inquired into whether there have been any new employees after the procedure was designed. | We have been informed that there have not been any new employees, after the procedure was designed, therefore we have not been able to test the implementation of the control.<br>No deviations noted. |

## A.14 Aquisition, development and maintenance of systems

### A.14.1 Security requirements of information systems

Control objective: To ensure that information security is an integrated part of information systems through the entire lifecycle. This also includes requirements of information systems, rendering services on public networks

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 14.1.1 | *Information security requirements analysis and specification*<br><br>The information security related requirements are being included in the requirements for new information systems or enhancements to existing information systems. | We have inspected the procedure for analysis and specification of information security requirements.<br><br>We have inspected a sample of implemented changes to determine whether requirements of security and controls in new information systems or in connection with existing systems have been described. | No deviations noted. |

### A.14.2 Security, development- and supporting processes

Control objective: To ensure that information security is planned and implemented with the development life cycle

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 14.2.1 | *Secure development policy*<br><br>Rules for the development of software and systems have been established and applied to developments within the organisation. | We have inspected the rules for developing software and systems.<br><br>We have, by sample test, inspected that the rules have been followed. | No deviations noted. |
| 14.2.2 | *Change control procedures*<br><br>Changes to systems within the development lifecycle are being controlled using formal change control procedures. | We have inspected the procedure for Change Management.<br><br>We have inspected a sample of changes, in order to establish whether the requirements to change management were followed. | No deviations noted. |

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 14.2.3 | *Technical review of applications after operating system changes*<br>When operating platforms are changed business critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security. | We have inspected the procedure for technical review of applications after operating system changes.<br>We have, by sample test, inspected that changes in operating systems and infrastructure have been evaluated regarding potential consequences to application systems, before being completed. | No deviations noted. |
| 14.2.5 | *Secure system engineering process*<br>Principles for engineering secure systems have been established, documented, maintained and applied to any information system implementation efforts. | We have inspected the procedure for system development.<br>We have, by sample test, inspected that the procedure has been followed. | No deviations noted. |
| 14.2.6 | *Secure development environment*<br>There is established appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle. | We have inspected the procedure for establishing a secure development environment.<br>We have inspected that access to the development environment is limited to employees with a work-related need for the access. | No deviations noted. |
| 14.2.8 | *System security testing*<br>Testing of security functionality is being carried out during development. | We have, by sample test, inspected that system security testing is performed as part of the system development process. | No deviations noted. |
| 14.2.9 | *System acceptance testing*<br>Acceptance testing programs and related criteria have been established for new information systems upgrades and new versions. | We have inquired about acceptance testing programs and related criteria for new information systems.<br>We have, on a sample basis, inspected that the patch level is up to date. | No deviations noted. |

| A.14.3 Test Data<br>Control objective: To ensure the protection of data used for testing. | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 14.3.1 | *Protection of test data*<br>Test data are being carefully selected, protected, managed and controlled. | We have inspected the procedure regarding selection and protection of test data. | No deviations noted. |

## A.15 Supplier relationships

| A.15.1 Information security in supplier relationships<br>Control objective: To ensure protection of the organisation's assets that are accessible by suppliers | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 15.1.1 | *Information security policy for supplier relationships*<br>Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets have been agreed with the supplier and documented. | We have inspected the procedure for closing agreements with subsuppliers. | No deviations noted. |
| 15.1.2 | *Addressing security within supplier agreements*<br>All relevant information security requirements are established and agreed with each supplier that may access process store communicate or provide IT infrastructure components for the company's information. | We have inspected the procedure for closing of agreement with subsuppliers.<br>We have inspected that the evaluation has been done for all subsuppliers. | No deviations noted. |

| 15.2 Supplier service delivery management<br>Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 15.2.1 | *Monitoring and review of third-party services*<br>Third-party services are monitored, reviewed and audited on a regular basis. | We have inquired if the procedure for monitoring and review of services from subsuppliers is according to the contract.<br>We have inspected that the subsuppliers have been risk assessed.<br>We have inspected that the review of third-party assurance reports for subsuppliers, are part of the annual wheel. | No deviations noted. |

# A.16 Information security incident management

| A.16.1 Management of information security incidents and improvements<br>Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 16.1.1 | *Responsibilities and procedures*<br>Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents. | We have inquired about the responsibilities and procedures of information security incidents.<br>We have inspected documentation for the distribution of responsibilities.<br>We have inspected the procedure for handling information security incidents. | No deviations noted. |
| 16.1.2 | *Reporting information security events*<br>Information security events are being reported through appropriate management channels as quickly as possible. | We have inspected the procedure for reporting on information security incidents.<br>We have, by sample test, inspected that incidents are handled in accordance with the procedure. | No deviations noted. |

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 16.1.3 | *Reporting security weaknesses*<br><br>Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services. | We have inspected the procedure for reporting security weaknesses.<br><br>We have inspected that awareness training is being held on a regular basis.<br><br>We have inquired into whether there have been any security weaknesses in the past year. | We have been informed that there have been no security weaknesses in the past year, therefore we are not able to test the implementation of the control.<br><br>No deviations noted. |
| 16.1.4 | *Assessment of and decision on information security events*<br><br>Information security events are assessed, and it is decided if they are to be classified as information security incidents. | We have inspected the procedure for assessment, response and evaluation of information security breaches. | No deviations noted. |
| 16.1.5 | *Response to information security incidents*<br><br>Information security incidents are responded to in accordance with the documented procedures. | We have, by sample test, inspected that information security incidents have been responded to, in accordance with the documented procedures. | No deviations noted. |
| 16.1.6 | *Learning from information security incidents*<br><br>Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents. | We have, by sample test, inspected that there is root-cause analysis of information security breaches in accordance with the procedure. | No deviations noted. |

## A.17 Information security aspects of business continuity management

### A.17.1 Information security continuity
Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 17.1.1 | *Planning information security continuity*<br>Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon. | We have inspected the business continuity plan. | No deviations noted. |
| 17.1.2 | *Implementing information security continuity*<br>Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented and maintained. | We have inspected that the business continuity plan is updated and approved. | No deviations noted. |
| 17.1.3 | *Verify review and evaluate information security continuity*<br>The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations. | We have inquired about procedures to ensure that all relevant systems are included in the continuity plan.<br>We have inspected that the test of the business continuity plan is planned in the annual wheel. | No deviations noted. |

| A.17.2 Redundancies<br>Control objective: To ensure availability of information processing facilities | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 17.2.1 | *Availability of information security processing facilities*<br>Information processing facilities have been implemented with redundancy sufficient to meet availability requirements. | We have inspected that the servers have been implemented with redundancy. | No deviations noted. |

## A.18 Compliance

| A.18.2 Information security reviews<br>Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures | | | |
|---|---|---|---|
| **No.** | **Pronestor ApS' control** | **Grant Thornton's test** | **Test results** |
| 18.2.1 | *Independent review of information security*<br>Processes and procedures for information security) (control objectives, controls, policies, processes and procedures for information security) are reviewed independently at planned intervals or when significant changes occur. | We have inspected, that independent evaluation of information security has been established. | No deviations noted. |
| 18.2.2 | *Compliance with security policies and standards*<br>Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements. | We have inquired the management's procedures for compliance with security policies and security standards.<br>We have inspected the annual wheel and how the internal controls are documented. | No deviations noted. |

| No. | Pronestor ApS' control | Grant Thornton's test | Test results |
|---|---|---|---|
| 18.2.3 | *Technical compliance review*<br><br>Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards. | We have inquired for internal controls to ensure compliance with security policies and procedures.<br><br>We have inspected the annual wheel and how the internal controls are documented. | No deviations noted. |

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."*

**Karsten Johan Busck**
**Underskriver 1**
*Serienummer: PID:9208-2002-2-989140174535*
*IP: 82.192.xxx.xxx*
*2022-11-03 08:37:32 UTC*
NEM ID

**Basel Obari**
**Underskriver 2**
*Serienummer: CVR:34209936-RID:99589866*
*IP: 188.179.xxx.xxx*
*2022-11-03 09:07:03 UTC*
NEM ID

**Jacob Helly Juell-Hansen**
**Underskriver 3**
*Serienummer: CVR:34209936-RID:50904197*
*IP: 62.243.xxx.xxx*
*2022-11-04 12:34:18 UTC*
NEM ID

*Penneo dokumentnøgle: GHWX7-VHEHW-WTKB3-C1KH1-JNE3O-T5MJC*