Grant Thornton

Assurance report

twoday A/S

ISAE 3402 type 2 assurance report on IT general controls for
the period from 1 May 2023 to 31 March 2024 related to Addo Sign

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

November 2024

Table of contents

Section 1: twoday A/S' statement

The accompanying description has been prepared for customers who have used twoday A/S' Addo Sign, 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. twoday A/S is using subservice organisation IT Relation A/S. This assurance report is prepared in accordance with the carve-out method and twoday A/S' description does not include control objectives and controls within IT Relation A/S. Certain control objectives in the description can only be achieved, if the subservice organisation's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control areas, stated in twoday A/S' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers are suitably designed and operationally effective with twoday A/S' controls. This assurance report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

twoday A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to twoday A/S' Addo Sign processing of customer transactions throughout the period from 1 May 2023 to 31 March 2024. 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 IT general 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 IT general controls

   (ii) Contains relevant information about changes in the IT general controls, performed during the period from 1 May 2023 to 31 March 2024

   (iii) 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 functioning during the period from 1 May 2023 to 31 March 2024 if relevant controls with the subservice organisation were operationally effective and the customers have performed the complementary user entity controls, assumed in the design of twoday A/S' controls throughout the period from 1 May 2023 to 31 March 2024. The criteria used in making this statement were that:

   (i) The risks that threatened achievement of the control objectives stated in the description were identified
   (ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved
   (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 May 2023 to 31 March 2024

Copenhagen, 18 November 2024
twoday A/S

Jesper Drustrup
Business Director, Products

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

To twoday A/S, their customers and their auditors.

Scope

We have been engaged to report on a) twoday A/S' description in Section 3 of its system for delivery of twoday A/S' Addo Sign throughout the period from 1 May 2023 to 31 March 2024 and the design and operational effectiveness of controls related to the control objectives stated in the description.

twoday A/S is using the subservice organisation IT Relation A/S. This assurance report is prepared in accordance with the carve-out method and twoday A/S' description does not include control objectives and controls within IT Relation A/S. Certain control objectives in the description can only be achieved if the subservice organisation's controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control objectives stated in twoday A/S' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with twoday A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

twoday A/S' responsibility

twoday A/S is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, twoday A/S 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 behaviour and ethical requirements applicable to Denmark.

Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on twoday A/S' description (Section 3) as well as on the design and operation 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 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 system, and the design and operating effectiveness 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 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 by the service organisation in Section 3.

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

twoday A/S' description in Section 3, 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 twoday A/S' statement in Section 1 and based on this, it is our opinion that:

(a) The description of the IT general controls, as they were designed and implemented throughout the period from 1 May 2023 to 31 March 2024, is fair in all material respects.

(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 May 2023 to 31 March 2024 in all material respects, if controls with subservice organisations were operationally effective and if the customers have designed and implemented the complementary user entity controls assumed in the design of twoday A/S' controls during the period 1 May 2023 to 31 March 2024

(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period from 1 May 2023 to 31 March 2024.

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 twoday A/S 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, 18 November 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Anders Holmgaard Christiansen State Authorised Public Accountant	Andreas Moos Director, CISA, CISM

Section 3: Description of twoday A/S' services in connection with operating of Addo Sign, and related IT general controls

Introduction

The following is a description of the Addo Sign service by twoday A/S. The report includes general processes and system setups etcetera with twoday A/S. Processes and system setups, individually agreed with Addo Sign customers, are not included in this report. Assessment of customer specific processes and system setups will be stated in specific assurance reports for customers who may have ordered such.

IT general controls at Addo Sign

The Addo Sign Service

The Addo Sign service is twoday A/S' general solution for the establishment of a more efficient process for digital signing of documents. The solution is delivered as software as service.

The solution covers the following areas:

- Upload documents and add recipient's information to send the documents to the recipient for signing or distribution.
- Print the documents using Addo Print directly to Addo Sign for processing.
- Import a PDF-document or a template with input data (XML-format) to be signed by the customer.
- Send documents to the recipients for digitally signing specifying the degree of assurance allowed for the signature. The levels supported are High (eIDAS), Substantial (MitID, Norwegian BankID, Swedish BankID and others) and Low, such as an electronic signature (touch) or the press of an "OK" button.
- Send the signer automatic reminders within the signing period.
- Distribute the digitally signed documents to all involved parties.
- Secure File Transfer (SFT). Secure distribution of files without signatures to various parties.
- Design simple forms using Addo Forms.
- Identity validation based on CPR lookup. This can only be done on Danish citizens.

Organisation and responsibilities

Addo Sign, the product, is a part of the twoday A/S group. As such, many of the more mundane tasks of running a company and the responsibilities thereof is handled on group level. Included in this list, but not limited to are:

- Housing
- Access to buildings and sites
- Onboarding to corporate systems such as time registration systems, reimbursement systems and such
- Corporate IT
- Handling of Data Protection processes

The responsibility and revision thereof are handled and described in the ISAE 3402 and ISAE 3000 done by the twoday A/S group and will not be included in this ISAE 3402.

Tasks which fall into the responsibility of Addo Sign and not directly handled by the twoday A/S group will be included in this ISA3402. Included in this list, but limited to are:

- Onboarding of new team members
- Risk management
- Data security & privacy

The above list is reviewed and controlled by the Addo Sign Product Steering committee.

Onboarding of new team members

Onboarding of new team members are handled jointly between the twoday A/S group and Addo Sign. The former takes care of onboarding the new team member into the corporate systems (time registration, reimbursement, salary etcetera). Addo Sign handles the onboarding of the new team member to the systems used while developing for or supporting the Addo Sign service.

Risk management

Revision and control of the risk log is done quarterly. Each item on the risk log is evaluated. Items which are no longer relevant are closed. Other items are re-assessed and possibly re-scored. The score of a risk denotes its severity of that risk. The severity of the risk should be seen in broadest possible way – the consequence of a risk happening may be anything from public defacement to processes not being properly followed.

An item on the risk log can have one of four states:

1. **Not started:** this is for newly identified items where no action has been taken.
2. **Started:** a risk item that is marked as started means that actual work is happening to mitigate the risk.
3. **On-going:** a risk item marked as on-going means that the risk at any time is present, and that the mitigation of the risk is impossible. This typically involves users and users' behavioural patterns.
4. **Closed:** the risk has been addressed and is no longer seen as a risk.

New risk items are added as seen fit. New risk items always start marked as "Not started."

Data security and privacy

The Addo Sign product team adheres strictly to the rules and processes as set forth in the EU GDPR. Access to data is controlled by layering of access right. The layers fall in these 3 broad categories:

- **Inner layer:** this is where only trusted Addo Sign personnel have access to the data.
- **Middle layer:** on this layer Addo Sign support personnel have access to be able to support our customers
- **Outer layer:** this is the layer where our customers have access to their own data.

No customer on the outer layer have access to other customer's data.

Access done on the middle layer (by the Addo Sign support personnel) is done through a specialised in-house developed interface controlling what kind of viewing / changes can be done.

Organisation of information security

Internal organisation

Addo Sign is a part of the twoday A/S group under the SaaS department. The director of the SaaS department, Jesper Drustrup, has the overall responsibility for the security policy of Addo Sign. This responsibility includes policies and procedures. All changes to the security policy must be approved by the SaaS department director.

Contact with authorities

Addo Sign has the necessary contact to the authority through the Divisional Security Officer/Divisional Data Protection Officer.

Information security as part of the product

We always take IT security into consideration in the Addo Sign product. All our developers are required to at least familiarise themselves with the best practices of the OWASP programme.

Furthermore, whenever security incident related news comes from CERT these are scrutinised and evaluated according to the software and configurations in the Addo Sign product.

Access control

Policies for access control in the product

Customers who sign up for a Addo Sign account online automatically becomes an administrator of the account. The customer administrators have the responsibility to create, maintain and disable access for their own users.

The customer can setup Two-/Multi Factor Authentication (2FA / MFA) on their users for enhanced security.

Management of user entries

User account rights

In Addo Sign there exist four different user accounts. From the most restrictive to the least restrictive rights these users are:

- **Standard User:** A standard user can only operate on the items the user creates.
- **Group Viewer:** A group viewer can operate on the items the user creates as well as having view only rights on other user's items belonging to the same group.
- **Group Administrator:** A group administrator can operate on all items in the group and do basic configuration of that group such as change templates.
- **Administrator:** A user with full administrative rights has access to the entire account and can do a full configuration of the account.

Handling of confidential logon information

Our IT security policy requires that our employees' passwords be personal.

User Responsibility

Use of confidential logon information

Our IT security policy requires that our employees' passwords be personal, and only the user knows the password. Password for system accounts is only known for a limited number of employees in the Addo Sign Team.

Control of access to systems and data

Restricted access to data

Our employee's user accounts are created with differentiated access rights and have only access to systems and data that is relevant to their work.

Procedures for secure log-on

All access to our systems requires user/password login.

Control of access to the source codes for programs

All employees with access to the code base have personal login to access and to add/change the code.

Safety of operation

Documented operating procedures

Addo Sign operating procedures are clearly described and communicated in the project guidelines for that reason that all new and current employees can fully understand and work with the system according to their qualifications. The guidelines cover the monitoring, safety, development, test and change management, and other operating procedures.

Despite the transparency of documented procedures roles and responsibilities, documentation underlines the specific key roles, who can execute the essential tasks.

These key roles indicate only experts with a robust technical expertise and historical knowledge, which needed to avoid the risk of unintended excess or damage to the system.

Change management

The procedure for change management is supported by the agile platform Jira from Atlassian software. The procedure ensures that all the changes are approved by the customer and/or internal experts as a part of optimisation process.

We have a standard change management model, which includes the following stages: pre-analysis and change description from the customer, solution, approval, test, and implementation. The project management team continuously monitors and assesses the changes to ensure timely implementation.

Changes and errors in operation servers are processed on the separate flow through IT Relation portal with a password-protected access.

Capacity controls

The capacity control of the server environment is conducted by IT Relation internally and reported to the Addo Sign project members via IT Relation portal.

Separation of development, test, and operational facilities

The Addo Sign project has the following operation facilities: operation and external environments, environment for the internal development and test environment.

The operation facilities are separated logically in accordance with the necessary access control to ensure that only authorised bodies can access the database and operation environment.

Protection against malware

Laptops and other development machines come preinstalled with Microsoft Defender for protection.

Access to twoday A/S' internal infrastructure from offsite must be done using a Cisco VPN client. As part of initiating the connection the Cisco VPN client downloads a scan profile. Access is allowed only if the scan profile is properly downloaded, executed and the result must show, that the client is free of malware.

Logging and monitoring

Logs can only be read by Addo Sign developers and IT Relation support personnel. Access is granted to these two personnel groups as they perform the day-to-day operations of the Addo Sign product.

The logs fall into two categories:

- **Addo Sign logs**. The Addo Sign logs contain information about runtime usage of the Addo Sign product. No sensitive data are logged in the logs. These logfiles are mainly used by the Addo Sign personnel and as they are product specific it requires insight into the inner workings of the product to derive anything meaningful from these logs.
- **Server logs**. The server logs contain what the OS logs. These logs are mainly used by IT Relation personnel, but they are also consulted by the Addo Sign personnel if incidents occur.

Time synchronisation

All servers are synchronised.

Control of technical vulnerabilities

All software products delivered by Addo Sign must be compliant with twoday A/S security policy.

The management of the technical vulnerabilities process is guided by risk management procedures focusing on timely identification of the risks associated with Addo Sign operation and an explicit recognition of unacceptable risk.

The risk management team and a technical officer must ensure that possible technical risks are continuously assessed, and the response actions developed.

Monitoring and evaluation of services from sub-processors

We have a procedure to ensure agreements and deliveries are met from sub-processor. Especially if audit reports must be obtained from sub-processors.

Management of incidents

Responsibilities and procedures

All employees are required to stay updated with the help of support websites, debate forums, respond to alarms from our systems and customers, partners, etc. to detect weaknesses. One must follow the rules applicable to reporting security incidents.

All security incidents must at least be examined and evaluated (in relation to our overall risk assessment model), at the quarterly meetings of the steering committee, and if there are serious threats should be evaluated immediately.

Reporting information security events

Our system for evaluating security events for clients as well as internal events allows us to prioritise incidents. The necessary actions can be handled upon the data from our security and risk log..

Our employees are required to report any security incident to the immediate supervisor as soon as possible to respond to events and necessary actions can be performed.

Assessment of information security breaches

We have a formal process for responding to security breaches. All security breaches are created in our task system, and we react immediately to the incident.

Responding to information security incidents

We have a formal process for responding to security incidents. All security incidents are created in our task system, and we react to the incident immediately.

Learning from information security breaches

All security incidents are part of our risk assessment, where we decide what actions we must implement to eliminate any vulnerabilities.

Emergency management

Contingency planning

The Addo Sign project has a business continuity plan to ensure that the Addo Sign functionality services provided, will be restored in time.

Implementation of emergency plans and procedures

The plan is tested as part of our emergency procedures, to ensure that we will experience a minimum of disruptions in operations in connection with any emergency. After completing the test, we analysed the results, and on this basis updated the relevant elements, procedures, and the business continuity plan.

Testing, maintenance, and review of emergency plans

Addo Sign performs a desk test of the plan annually.

Redundancy

There is established the necessary redundancy at our hosting partner to meet accessibility requirements in production.

Conformity

Independent evaluation of information security

The security function in twoday A/S continuously performs an audit on all our activities.

Once an independent IT auditor reviews a year Addo Sign, to submit a 3402 statement of compliance controls mentioned in this control description.

Compliance with security policies and security standards

twoday A/S secure anchoring of the IT security policy by all employees by annually review.

Checking technical compliance

twoday A/S distributes information to all employees about our IT security policies, rules, and procedures. Additionally, there are educational programs for IT security to ensure that there is understanding and compliance with rules and procedure.

Changes in IT use or control environment

Significant changes in infrastructure or control environment from 1 May 2023 to 31 March 2024:

We changed hosting partner from IT Relation to Cloud Factory which have changed our processes from being managed by 3rd party to be in full control ourselves.

Complementary user entity controls with customers

Prerequisites regarding the customers' responsibilities are described in individual contracts and agreement manuals. It is noted that customers who sign up for a Addo Sign account online automatically becomes an administrator of the account. The customer administrators have the responsibility to enable and disable accounts for their own users. Customers are responsible for configuring password settings in Addo Sign based on the functionality made available by Twoday.

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

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 twoday A/S' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by twoday A/S' customers, are not included in this report.

Tests performed

We performed our test of controls at twoday A/S, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at twoday A/S regarding controls. Inquiries have included questions on how controls are being performed.
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. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with twoday A/S.

A.5 Information security policies

A.5.1 Management direction for information security
Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

No.	*twoday A/S' control*	*Grant Thornton's test*	*Test results*
5.1.1	*Policies for information security* 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 that the information security policy has been approved by management, published, and communicated to employees. We have inspected that the information security policy has been reviewed and approved by the management.	No deviations noted.
5.1.2	*Review of policies for information security* 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 inquired into the procedure for regular review of the information security policy. We have inspected that the information security policy is reviewed, based on updated risk assessments to ensure that it still is suitable, adequate, and efficient.	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.	twoday A/S' control	Grant Thornton's test	Test results
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected an organisation chart showing the information security organisation. We have inspected that the structure is sufficient to manage the implementation and operation of information security. We have inspected the description of roles and responsibilities within the information security organisation.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisations' assets.	We have inspected documentation of segregation of duties. We have inspected general organisation chart for the organisation.	No deviations noted.

A.6.2 Mobile devices and teleworking

Control objective: To ensure the security of teleworking and use of mobile devices

No.	twoday A/S' control	Grant Thornton's test	Test results
6.2.1	*Mobile device policy* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected policy for securing of mobile devices. We have inspected that relevant employees have been informed about the mobile device policy. We have inspected, that technical controls for securing of mobile devices have been defined.	No deviations noted.

No.	twoday A/S' control	Grant Thornton's test	Test results
6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected the policy for securing of remote workspaces. We have inspected the underlaying 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.	twoday A/S' control	Grant Thornton's test	Test results
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities in information security.	We have inspected the procedure for onboarding new employees. We have, by sample test, inspected documentation that new employees have been informed about their roles and responsibilities in information security.	No deviations noted.

A.7.2 During employment

Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities

No.	twoday A/S' control	Grant Thornton's test	Test results
7.2.1	*Management responsibility* 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 information security policy for establishing requirements for employees and contractors. We have inspected, that the management, in contracts, has required that employees and contractors must observe the information security policy.	No deviations noted.

No.	twoday A/S' control	Grant Thornton's test	Test results
7.2.2	*Information security awareness education and training* 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 inspected procedures for ensuring adequate education and information security training (awareness training) We have inspected that activities to develop and maintain employees' security awareness have been carried out.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected that a formal disciplinary process has been established and communicated to employees and contractors. We have, by sample test, inspected that the disciplinary process is an integrated part of the employment contract.	No deviations noted.

A.7.3 Termination and change of employment
Control objective: To protect the organisation's interests as part of the process of changing or terminating employment

No.	twoday A/S' control	Grant Thornton's test	Test results
7.3.1	*Termination or change of employment responsibility* 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 or contract. We have inspected documentation that information security responsibilities and duties that remain valid after termination or change of employment have been defined and communicated. We have, by sample test, inspected that resigned employees are being informed that confidentiality agreement is still valid after termination of contract.	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets

Control objective: To identify organisational assets and define appropriate protection responsibilities

No.	twoday A/S' control	Grant Thornton's test	Test results
8.1.1	*Inventory of assets* 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 asset listings.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected list of asset ownership.	No deviations noted.
8.1.3	*Acceptable use of assets* 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 rules for acceptable use of assets.	No deviations noted.
8.1.4	*Return of assets* 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 ensuring return of assets. We have, by sample test, inspected that assets are being returned from terminated employees.	No deviations noted.

A.9 Access control

A.9.1 Business requirements of access control
Control objective: To limit access to information and information processing facilities

No.	twoday A/S' control	Grant Thornton's test	Test results
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inspected the access control policy. We have inspected that the policy has been reviewed and approved by management.	No deviations noted.
9.1.2	*Access to network and network services* Users are only being provided with access to the network and network services that they have been specifically authorised to use.	We have inspected that a procedure for granting access to network and network services has been established. We have inspected list of users with access to network and network services. We have inquired into whether access is based on the employees' work-related needs.	No deviations noted.

A.9.2 User access management
Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	twoday A/S' control	Grant Thornton's test	Test results
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected that formalised procedures for user registration and de-registration have been established. We have inquired into whether new user access rights have been created during the audit period. We have inspected that resigned users' access rights have been revoked.	We have been informed that there have been no new user accounts added to the Addo system during the audit period. No deviations noted

No.	twoday A/S’ control	Grant Thornton’s test	Test results
9.2.2	*User access provisioning* 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. We have inquired whether new user access rights have been created in the audit period. We have inquired into whether any users have changed roles or jobs during the period.	We have been informed that there have been no new user accounts added to the Addo system during the audit period. No deviations noted
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected the procedures for allocation, use and restrictions of privileged access rights. We have inspected a list of privileged users and inquired into whether access rights have been allocated based on a work-related need. We have inspected that privileged user accesses are personally identifiable. We have inspected, that periodical review of privileged access rights is being performed.	No deviations noted.
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have inspected the procedure regarding allocation of access codes to platforms. We have inspected documentation that the password policy is implemented in systems used to manage secret authentication information about users.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user’s access rights at regular intervals	We have inspected the procedure for regular review and assessment of access rights. We have inspected, that review and assessment of access rights is being performed twice a year.	No deviations noted.
9.2.6	*Removal or adjustment of access rights* 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 inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that resigned employees have had their access rights cancelled.	No deviations noted.

A.9.3 User responsibilities
Control objective: To make users accountable for safeguarding their authentication information

No.	twoday A/S' control	Grant Thornton's test	Test results
9.3.1	*Use of secret authentication information.* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected guidelines for use of secret passwords. We have inspected, that twoday has implemented password functionality that allows customers to configure their own password settings.	No deviations noted.

A.9.4 System and application access control
Control objective: To prevent unauthorised access to systems and applications

No.	twoday A/S' control	Grant Thornton's test	Test results
9.4.2	*Secure logon procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected the procedure for secure logon. We have inspected, that MFA has been established in connection with logon.	No deviations noted.
9.4.5	*Access control to program source code* Access to program source code has been restricted.	We have inquired into procedures for restricting access to program source codes. We have inspected, that access to source codes has been limited to employees with a work-related need.	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.	*twoday A/S' control*	*Grant Thornton's test*	*Test results*
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy for the use of encryption. We have inspected list of updates and review of policies, and procedures where the policy for cryptography is included.	No deviations noted.
10.1.2	*Key Management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, which supports the company use of cryptographic techniques. We have inspected that cryptographic keys are active, and that their renewal is being followed up on.	No deviations noted.

A.11 Physical and environmental security

A.11.1 Secure areas

Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

No.	*twoday A/S' control*	*Grant Thornton's test*	*Test results*
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected the procedure for physical protection of facilities and security perimeters. We have inspected relevant locations and their security perimeters to establish whether security measures have been implemented to prevent unauthorised access.	No deviations noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access.	We have inspected access points to establish, whether personal access cards are used to gain access to the office. We have inspected that alarms have been installed for physical access control.	No deviations noted.

No.	*twoday A/S' control*	*Grant Thornton's test*	*Test results*
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inspected that physical security has been applied to protect offices, rooms, and facilities. We have inspected that fire alarms are installed on the office.	No deviations noted.

A.11.2 Equipment
Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

No.	*twoday A/S' control*	*Grant Thornton's test*	*Test results*
11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	We have inspected the procedure for protection of unattended equipment.	No deviations noted.
11.2.9	*Clear desk and clear screen policy.* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.	We have inquired into the policy of tidy desk and clear screen. We have inspected documentation that lock screen timeout is active and follows the policy for clear screen.	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.	twoday A/S' control	Grant Thornton's test	Test results
12.1.3	*Capacity management* 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 inspected the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements We have inspected documentation for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements We have inspected that alarms are active and continuously reviewed.	No deviations noted.
12.1.4	*Separation of development-, test- and operations facilities.* Development testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.	We have inspected technical documentation that used system environments have been separated.	No deviations noted.

A 12.2 Protection from malware

Control objective: To ensure that information and information processing facilities are protected against malware

No.	twoday A/S' control	Grant Thornton's test	Test results
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inspected guidelines for controls against malware. We have inspected that controls against malware have been implemented.	No deviations noted.

A.12.4 Logging and monitoring
Control objective: To record events and generate evidence

No.	twoday A/S' control	Grant Thornton's test	Test results
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inquired into logging of user activities. We have inspected that logging configurations contain user activities, exceptions, faults, and incidents.	No deviations noted.
12.4.4	*Clock synchronisation* 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 inquired into procedures for synchronisation against a reassuring time server. We have inspected, that synchronisation against a reassuring time server, has been implemented.	No deviations noted.

A.12.6 Technical vulnerability management
Control objective: To prevent exploitation of technical vulnerabilities

No.	twoday A/S' control	Grant Thornton's test	Test results
12.6.1	*Management of technical vulnerabilities* 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 inspected the procedure regarding gathering and evaluation of technical vulnerabilities. We have, by sample test, inspected that servers, database systems and network components are patched in time.	No deviations noted.

A.15 Supplier relationships

15.2 Supplier service delivery management

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

No.	twoday A/S' control	Grant Thornton's test	Test results
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inspected that the procedure for managing suppliers and supplier agreements contains requirements of yearly monitoring and review of services rendered, are according to the contract. We have inspected, that review and assessment of relevant audit reports on significant subservice organisations have been performed.	No deviations noted.
15.2.2	*Manage changes to the third-party services* Changes in supplier services, including maintenance and improvement of existing information security policies, procedures, and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have inquired about management of changes with the subservice organisation, and we have inspected the documentation for handling this.	We have been informed that there have been no changes in the suppliers during the assurance period. No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements

Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

No.	*twoday A/S' control*	*Grant Thornton's test*	*Test results*
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inspected the procedure for manging security incidents. We have inspected that the procedure has been reviewed and updated during the period.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inspected guidelines for reporting of information security incidents. We have inquired whether the information security incidents are being reported through appropriate management channels.	We have been informed that no incidents, events, or breaches has occurred during the audit period. No deviations noted.
16.1.3	*Reporting security weaknesses* 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 guidelines for reporting of information security weaknesses. We have inquired whether the employees have reported weaknesses or suspected weaknesses in information systems and services.	We have been informed that no incidents, events, or breaches has occurred during the audit period. No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inspected procedure for assessment of information security incidents. We have inquired whether the information security incidents have been managed according to the procedure.	We have been informed that no incidents, events, or breaches has occurred during the audit period. No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inspected the procedure for managing information security breaches. We have inquired into whether information security breaches have occurred during the period.	We have been informed that no incidents, events, or breaches has occurred during the audit period. No deviations noted.

No.	twoday A/S' control	Grant Thornton's test	Test results
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about problem-management function which analyses information security beaches in order to reduce probability of recurrence. We have inquired whether the experience from information security breaches is handled.	We have been informed that no incidents, events, or breaches have occurred in the audit period. 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.	twoday A/S' control	Grant Thornton's test	Test results
17.1.1	*Planning information security continuity* 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 that the contingency plan has been approved by management. We have inspected that the contingency plan has been prepared, based on a risk assessment.	We have inspected that there is a general contingency plan for twoday A/S, but not a specific emergency plan for Addo Sign. We have been informed that the specific contingency plan for Addo Sign is being prepared. No further deviations noted.
17.1.2	*Implementing information security continuity* 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 contingency plan is maintained and updated as needed. We have inspected documentation that the contingency plan is accessible to relevant employees.	We have inspected that there is a general contingency plan for twoday A/S, but not a specific emergency plan for Addo Sign. We have been informed that the specific contingency plan for Addo Sign is being prepared. No further deviations noted.

No.	twoday A/S' control	Grant Thornton's test	Test results
17.1.3	*Verify review and evaluate information security continuity* 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 inspected documentation that risk areas in the contingency plan have been tested during the period.	We have inspected that the general contingency plan for twoday A/S has been tested, but not a specific emergency plan for Addo Sign, as this plan is being prepared. No further deviations noted.

A.18 Compliance

A.18.2 Information security reviews
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures

No.	twoday A/S' control	Grant Thornton's test	Test results
18.2.1	*Independent review of information security* 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 documentation that independent review of the information security has been performed.	No deviations noted.

The signatures in this document are legally binding. The document is signed with Addo Sign secure digital signature.
The signer's identity is physically registered in the electronic PDF document and shown below.
All times are given in Coordinated Universal Time (UTC).

Signers

Jesper Drustrup
Business Director - Products
3b4262e0-7ea4-426a-89da-fc3db7c4c385 *2024-11-18 10:45:26Z*

Andreas Moos
Director | IT Risk Assurance & Advisory Services
eace5ed6-cfa7-4d9e-b982-120d10f47204 *2024-11-18 10:48:06Z*

Anders Holmgaard Christiansen
Partner
250abf98-7048-42a1-8db3-222c9125bb0e *2024-11-18 11:01:23Z*

Documents in the transaction

twoday - Addo Sign - ISAE 3402-II - 2024 - Assurance Report.pdf *SHA256: 5c2d94dc129eb6c61871095a7ea6e533dd8e7c24af553803b64fa70e5cb6a761*

Addo Sign identification number: 32aebc3b-653e-4adb-b19c-2623eb32c56a

Addo Sign

The document is digitally signed with the Addo Sign secure signing service. The signature evidence in the document is secured and validated using the mathematical hash value of the original document.

The document is locked for changes and time-stamped with a certificate from a trusted third party. All cryptographic signing proofs are embedded in the PDF document in case they are to be used for validation in the future.

How to verify the authenticity of the document
The document is protected with an Adobe CDS certificate. When the document is opened in Adobe Reader, it will appear to be signed with the Addo Sign signing service.