



Assurance report

twoday A/S

ISAE 3402 type 2 assurance report on IT general controls for the period 1 May 2022 to 30 April 2023 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 2023

Table of contents

| | | |
|------------|---|----|
| Section 1: | twoday A/S' statement | 1 |
| Section 2: | Independent service auditor's assurance report on the description of controls, their design and operating effectiveness | 3 |
| Section 3: | Description of twoday A/S' services in connection with operating of Addo Sign, and related IT general controls | 6 |
| Section 4: | Control objectives, controls, and service auditor testing | 15 |

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 subsupplier's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subsuppliers.

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 controls with the customers (or the specific customer) are suitably designed and operationally effective with twoday A/S' controls. This assurance report does not include the appropriateness of the design and operational effectiveness of these complementary 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 1 May 2022 to 30 April 2023. 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 1 May 2022 to 30 April 2023
 - (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 operationally effective during the period 1 May 2022 to 30 April 2023 if relevant controls with the sub-supplier were operationally effective and the customers have performed the complementary controls, assumed in the design of twoday A/S' controls throughout the period from 1 May 2022 to 30 April 2023. 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 used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, throughout the period from 1 May 2022 to 30 April 2023

Copenhagen, 27 November 2023
twoday A/S

Jesper Drustrup
Director, COO

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 twoday A/S' description in Section 3 of its system for delivery of a) twoday A/S' services in accordance with the data processing agreement with customers as data controllers throughout the period 1 May 2022 to 30 April 2023 and about b+c) the design and operating effectiveness of controls related to the control objectives stated in the description.

twoday A/S is using subservice organisations 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 subsupplier's controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subsuppliers.

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 controls with the customers (or the specific customer) have been appropriately designed and operationally effective with the controls with twoday A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

twoday A/S' responsibility

twoday A/S is responsible for preparing the description in Section 3 and accompanying statement in 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 Control 1¹ 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.

Auditor's responsibility

Our responsibility is to express an opinion on twoday A/S' description in Section 3 as well as on the design and operating effectiveness of controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by 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 1 May 2022 to 30 April 2023, is fair in all material respects.
- (b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 May 2022 to 30 April 2023 in all material respects, if controls with subsuppliers were operationally effective and if the customers have designed and implemented the complementary controls assumed in the design of twoday A/S' controls during the period 1. April 2022 to 30. April 2023.
- (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 1 May 2022 to 30 April 2023.

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 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 to the financial reporting.

Copenhagen, 27 November 2023

Grant Thornton

Godkendt Revisionspartnerselskab

Jacob Helly Juell-Hansen
State Authorised Public Accountant

Basel Rimon Obari
Executive 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.

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.

Organization 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
- Vendor management

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 & 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 rights. 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 specialized in-house developed interface controlling what kind of viewing / changes can be done.

Vendor management

Yearly the Addo Sign team evaluates our vendor list. Each vendor is evaluated based on the following premises:

- Do they comply with the GDPR?
- Do they have a sufficient level of security built into their service rendered to us?

Where applicable we evaluate their ISAE 3402 and ISAE 3000 statements. Vendors not giving us sufficient information will end up in our risk log.

Organization of information security

Internal organization

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.

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 familiarize themselves with the best practices of the OWASP programme.

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

Mobile devices and remote workplaces

The terms of use for all equipment, mobile or stationary is a part of the twoday A/S security policy. All employees have participated in security sessions to give awareness about how to behave when working at twoday A/S.

Policy for mobile devices

We ensure through the latest standards for security solutions to secure mobile equipment like laptops and mobile phones etc.

All devices are secured in case of physical loss by encryption and password protection.

Remote Workstations

Remote access is secured by VPN connections, and the policy for using mobile and Remote Access is a part of our security policy.

Security in relation to HR

All employees at twoday A/S including the Addo Sign team are regulated by the company rules described in the Employee Handbook.

Employment

Terms of employment, including confidentiality on their own and clients' conditions are described in the employee's contract of employment.

Recruitment

When hiring, new employees sign a contract. In the contract is contained, that the employee must meet the all-time policies and procedures.

In connection with the use of external suppliers who have access to our systems, we ensure the conclusion of confidentiality agreements.

Awareness, education, and training in information security

Our assets are very much our employees, and we ensure that our employees receive continuous training. This is done by sharing internal knowledge, and relevant external courses and certifications. We have an annual review of our security policy, where it is reviewed. Employees are recorded by participation.

Our security information ISMS is at any time available to all employees on the company intranet.

Termination or changes in employment

General arrangements for the recruitment, including conditions related to termination of employment described in the Staff Handbook.

Management is responsible for ensuring that the employee is informed of the present rules during and after employment.

Asset management

List of assets

Our networks and the environment are complex with many systems and customers, and to protect against unauthorized access, and to ensure the transparency of the building, we have designed a range of documentation describing the internal network, devices, device naming, logical partitioning, etc.

Ownership of assets

We work in twoday A/S with ownership of assets to ensure that no units, systems, or data will be forgotten in terms of security updates, backup, development, and maintenance.

Acceptable use of assets

The acceptable use of twoday A/S assets is described in the ISMS handbook on the company intranet.

Return of assets

Upon termination of employment, we have a detailed procedure to be followed to ensure that employees deliver all relevant assets, including portable media etc.

Access control

twoday A/S have a policy for access control both physically and logically. The policy is part of our IT security standard.

Business requirements for access control

All employees at twoday A/S gets a personal key card to use for accessing the building. Outside office hours, employees must use a personal pin code together with the key card to access the building.

The building has a reception who register visitors in normal opening hours. The reception staff administrate the key card.

The administration of access to twoday A/S both physically and logically is an integrated part of the on/off boarding process.

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.

Access to networks and network services

twoday A/S

Access to twoday A/S network is restricted by a personal network account. Each network account has only necessary rights to access network resources depending on the individual employee's tasks. The support department administers the network rights.

IT Relation

All production data for Addo Sign is located at our hosting partner IT Relation. IT Relation and Addo Sign has a documented procedure for accessing servers and data for Addo Sign at IT Relation.

Termination of employee

The employee's access to network and E-mail accounts are closed upon termination of employment, as well as physical access and access to systems at twoday A/S and subsuppliers.

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 are personal.

User Responsibility

Use of confidential logon information

Our IT security policy requires that our employees' passwords are 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 has 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.

Cryptography

Control of the use of cryptography

Addo Sign uses strong cryptography for safe communication. All communication between components in the system is done over encrypted lines.

E-mails sent from the system are protected by the highest level of TLS the receiving system is ready to accept.

Web-traffic to the system is encrypted using HTTPS (TLS).

Cryptography policy

When it is technically possible, Addo Sign is using leading industrial cryptography to secure communication. For example:

- Mail signing certificate
- Server SSL certificates
- SMTP server TLS certificate
- VPN connections between Addo Sign and customers

Managing encryption keys

We have a process for maintaining and updating cryptography.

Physical and environmental security

Physical security

twoday A/S has secure office facilities with no access for unauthorized persons.

Physical access control

To access our offices, you must use a personal employee key card or contact our reception within office hours. Our reception registers all visitors.

Should external persons (suppliers or customers) have access to our facilities, they must be accompanied by an employee.

Securing offices, rooms, and facilities

All our rooms are fitted with a burglar alarm that in case of intrusion alert the private security company, as well as relevant people with twoday A/S via SMS and e-mail.

Unauthorized persons will not be able to walk freely around in our offices, as our reception is staffed, and other external doors are locked.

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.

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 authorized 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.

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 contains information about runtime usage of the Addo Sign product. No sensitive data is 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 synchronization

All servers are synchronized.

Control of technical vulnerabilities

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

The management of 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, discussion 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 prioritize incidents. The necessary actions can be handled upon the data from our security and risk log. Reporting security weaknesses

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 immediately to the incident.

Learning from information security breaches

All security incidents are part of our risk assessment, which we decide on 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 Business Continuity Plan.

Testing, maintenance, and review of emergency plans

Addo Sign performs a desk test of the plan annually.

Redundancy

The necessary redundancy is established 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 a year Addo Sign is reviewed by an independent IT auditor, 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 for the period:

- No changes to infrastructure

Complementary Controls

User enabling/disabling

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.

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. |

Addo Sign identifikationsnummer: a5f68011-2733-4405-ae7b-965a259dbc64

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 | <p><i>Policies for information security</i></p> <p>A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.</p> | <p>We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant external parties.</p> <p>We have inspected the risk assessment and ensured that it follows the procedure for handling risks.</p> | No deviations noted. |
| 5.1.2 | <p><i>Review of policies for information security</i></p> <p>The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.</p> | <p>We have inspected the information security policy and ensured that it is updated during the period.</p> <p>We have inspected the risk assessment and ensured that it is updated during the period.</p> | 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 | <p><i>Information security roles and responsibilities</i></p> <p>All information security responsibilities are defined and allocated.</p> | We have inspected documentation that responsibility for information security is clearly defined and distributed. | No deviations noted. |
| 6.1.2 | <p><i>Segregation of duties</i></p> <p>Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.</p> | We have inspected the guidelines for separation of functions, and we have, by sample test, inspected documentation for implementation of the guidelines. | 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 | <p><i>Mobile device policy</i></p> <p>Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.</p> | <p>We have inspected mobile device security policy.</p> <p>We have, by sample test, inspected documentation for the implementation of technical controls on mobile devices.</p> | No deviations noted. |
| 6.2.2 | <p><i>Teleworking</i></p> <p>Policy and supporting security measures are implemented to protect information accessed, processed and stored at teleworking sites.</p> | We have inspected policy for securing remote workplaces and we have inspected underlying security measures to protect remote workplaces in accordance with internal policy. | No deviations noted. |

A.7 Human resource 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 | <p><i>Terms and conditions of employment</i></p> <p>The contractual agreements with employees and contractors are stating their and the organisation's responsibilities in information security.</p> | <p>We have inspected guidelines for employees and ensured that employees are obliged to follow them.</p> <p>We have, by sample test, inspected employees who joined during the period, and by sample test ensured that new employees have signed an employment agreement.</p> <p>We have, by sample test, inspected employees who joined during the period, and by sample test checked that new employees have followed the onboarding process.</p> | <p>We have observed that for one out of ten samples, it has not been possible to obtain an employment contract.</p> <p>We have observed that for three out of ten samples, it has not been possible to document the onboarding process, and for one out of eight samples parts of the onboarding process were not completed.</p> <p>No further deviations noted.</p> |

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 | <p><i>Management responsibility</i></p> <p>Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.</p> | <p>We have, by sample test, inspected contracts, and by sample test checked that employees are obliged to comply with the personnel handbook.</p> | <p>No deviations noted.</p> |
| 7.2.2 | <p><i>Information security awareness education and training</i></p> <p>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.</p> | <p>We have inspected that activities have been carried out to develop and maintain safety awareness among employees.</p> | <p>No deviations noted.</p> |

| No. | twoday A/S' control | Grant Thornton's test | Test results |
|-------|---|---|----------------------|
| 7.2.3 | <p><i>Disciplinary process</i></p> <p>There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.</p> | We have inspected the policy for sanctions. | 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 | <p><i>Termination or change of employment responsibility</i></p> <p>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.</p> | We have inquired about resigned employees during the period. | <p>We have been informed that no employees have resigned during the period for Addo Sign, why we have not tested the effectiveness of the control.</p> <p>No deviations noted.</p> |

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 | <p><i>Inventory of assets</i></p> <p>Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.</p> | We have, by sample test, inspected lists of assets including devices, internal network, and servers. | No deviations noted. |

Addo Sign identifikationsnummer: a5f68011-2733-4405-ae7b-965a259dbc64

| <i>No.</i> | <i>twoday A/S' control</i> | <i>Grant Thornton's test</i> | <i>Test results</i> |
|------------|--|--|--|
| 8.1.2 | <p><i>Ownership of assets</i></p> <p>Assets maintained in the inventory are being owned.</p> | <p>We have inspected that the owner of assets appears in the lists of assets.</p> <p>We have, by sample test, inspected new employees during the period, and by sample test checked that they appear as the owner of their assets.</p> | No deviations noted. |
| 8.1.3 | <p><i>Acceptable use of assets</i></p> <p>Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.</p> | We have inspected that there are guidelines for acceptable use of assets. | No deviations noted. |
| 8.1.4 | <p><i>Return of assets</i></p> <p>All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.</p> | We have, by sample test, inspected resignations during the period, and by sample test checked that the offboarding procedure has been followed, including handing over assets. | <p>We have observed that one out of six samples have not followed the offboarding procedure.</p> <p>No further deviations noted.</p> |

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 | <p><i>Access control policy</i></p> <p>An access control policy has been established, documented, and reviewed based on business and information security requirements.</p> | <p>We have inspected the policy for access control and ensured that requirements for access management have been established.</p> | <p>We have observed that the access policy was last approved in 2021.</p> <p>No further deviations noted.</p> |
| 9.1.2 | <p><i>Access to network and network services</i></p> <p>Users are only being provided with access to the network and network services that they have been specifically authorized to use.</p> | <p>We have inspected that a procedure has been established for granting access to networks and network services.</p> <p>We have, by sample test, inspected registration and de-registration of users to the internal network.</p> | <p>No deviations noted.</p> |

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 | <p><i>User Registration and de-registration</i></p> <p>A formal user registration and de-registration process has been implemented to enable assignment of access rights.</p> | <p>We have inspected that there are formalized procedures for assigning and cancelling users' access rights.</p> <p>We have, by sample test, inspected the allocation and de-registration of users.</p> | <p>No deviations noted.</p> |

| No. | twoday A/S' control | Grant Thornton's test | Test results |
|------------|--|---|----------------------|
| 9.2.2 | <p><i>User access provisioning</i></p> <p>A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services</p> | <p>We have inspected that there are formalized procedures for assigning and cancelling users' access rights.</p> <p>We have, by sample test, inspected the allocation and de-registration of users.</p> | No deviations noted. |
| 9.2.3 | <p><i>Management of privileged access rights</i></p> <p>The allocation and use of privileged access rights have been restricted and controlled.</p> | <p>We have inspected documentation for review of privileged users during the period.</p> <p>We have, by sample test, inspected privileged user accesses to internal systems.</p> | No deviations noted. |
| 9.2.4 | <p><i>Management of secret-authentication information of users</i></p> <p>The allocation of secret authentication information is controlled through a formal management process.</p> | <p>We have inspected the guidelines for assigning secret authentication information.</p> | No deviations noted. |
| 9.2.5 | <p><i>Review of user access rights.</i></p> <p>Asset owners are reviewing user's access rights at regular intervals</p> | <p>We have inspected documentation for review of user access during the period.</p> | No deviations noted. |
| 9.2.6 | <p><i>Removal or adjustment of access rights</i></p> <p>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.</p> | <p>We have inspected that there are procedures in place for assigning and adjusting users' access rights.</p> <p>We have, by sample test, inspected the allocation and de-registration of users.</p> | 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 | <p><i>Use of secret authentication information.</i></p> <p>Users are required to follow the organisations' s practices in the use of secret authentication information.</p> | We have, by sample test, inspected passwords, and by sample test ensured that this is in accordance with internal policy. | 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 | <p><i>Secure logon procedures</i></p> <p>Access to systems and applications is controlled by procedure for secure logon.</p> | We have, by sample test, inspected documentation that systems require unique user-ID and password. | No deviations noted. |
| 9.4.3 | <p><i>Password management system</i></p> <p>Password management systems are interactive and have ensured quality passwords.</p> | We have, by sample test, inspected passwords and ensured that it is compliant with an internal policy. | No deviations noted. |
| 9.4.5 | <p><i>Access control to program source code</i></p> <p>Access to program source code has been restricted.</p> | We have inspected users with access to source code and ensured that users have a personal login. | 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 | <p><i>Policy on the use of cryptographic controls</i></p> <p>A policy for the use of cryptographic controls for protection of information has been developed and implemented.</p> | We have, by sample test, inspected encryption of information, and by sample test ensured that this is implemented according to internal policy. | No deviations noted. |
| 10.1.2 | <p><i>Key Management</i></p> <p>A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.</p> | We have, by sample test, inspected that certificates are handled in accordance with internal policy. | 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 | <p><i>Physical security perimeter</i></p> <p>Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.</p> | <p>We have inspected that there are guidelines for physical security.</p> <p>We have, by sample test, inspected the physical access control.</p> | No deviations noted. |
| 11.1.2 | <p><i>Physical entry control</i></p> <p>Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.</p> | We have, by sample test, inspected the physical access control and by sample test checked that this is in accordance with the guidelines. | No deviations noted. |

| No. | twoday A/S' control | Grant Thornton's test | Test results |
|------------|--|--|-----------------------------|
| 11.1.3 | <p><i>Securing offices, rooms, and facilities</i></p> <p>Physical security for offices rooms and facilities has been designed and applied.</p> | <p>We have, by sample test, inspected documentation that there is access control in relation to the supplier's office.</p> | <p>No deviations noted.</p> |

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 | <p><i>Unattended user equipment</i></p> <p>Users are ensuring that unattended equipment has appropriate protection.</p> | <p>We have inspected the policy for safeguarding unattended equipment.</p> <p>We have, by sample test, inspected documentation that the policy has been implemented.</p> | <p>No deviations noted.</p> |
| 11.2.9 | <p><i>Clear desk and clear screen policy.</i></p> <p>A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.</p> | <p>We have inspected the clean desk and blank screen policy.</p> <p>We have, by sample test, inspected that blank screen is turned on.</p> <p>We have inspected documentation that clean desk has been implemented.</p> | <p>No deviations noted.</p> |

Addo Sign identifikationsnummer: a5f68011-2733-4405-ae7b-965a259dbc64

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 | <p><i>Capacity management</i></p> <p>The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.</p> | <p>We have, by sample test, inspected documentation for that twoday has received report in regard to capacity of the server environment during the period.</p> | <p>No deviations noted.</p> |
| 12.1.4 | <p><i>Separation of development-, test- and operations facilities.</i></p> <p>Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.</p> | <p>We have, by sample test, inspected documentation that development and operational environments are separated.</p> | <p>No deviations noted.</p> |
| 12.2.1 | <p><i>Control against malware</i></p> <p>Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.</p> | <p>We have, by sample test, inspected documentation for implementation of controls against malware on local machines.</p> | <p>No deviations noted.</p> |

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 | <p><i>Event logging</i></p> <p>Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.</p> | We have, by sample test, inspected event logging on applications and on system level. | No deviations noted. |
| 12.4.4 | <p><i>Clock synchronization</i></p> <p>The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.</p> | We have inspected documentation for NTP. | 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 | <p><i>Management of technical vulnerabilities</i></p> <p>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.</p> | We have inspected the risk assessments and ensured that technical risks have been addressed. | 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 | <p><i>Monitoring and review of third-party services</i></p> <p>Organisations are regularly monitoring review and audit supplier service delivery.</p> | <p>We have inspected the procedure for managing suppliers and ensured that there is a requirement for continuous supervision of suppliers.</p> <p>We have inspected documentation that supervision was carried out during the period.</p> | <p>We have been informed that the procedure for dealing with suppliers has not been updated during the period.</p> <p>No further deviations noted.</p> |
| 15.2.2 | <p><i>Manage changes to the third-party services</i></p> <p>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.</p> | <p>We have inspected the procedure for changing sub-suppliers.</p> <p>We have inquired about changed sub-suppliers during the period.</p> | <p>We have been informed that there have been no changes in suppliers during the period, which is why we have not been able to test the effectiveness of the control.</p> <p>No deviations noted.</p> |

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 | <p><i>Responsibilities and procedures</i></p> <p>Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.</p> | <p>We have inspected procedures for incident handling and ensured that responsibilities and methods for handling incidents are described.</p> | <p>We have observed that one procedure for handling incidents has been approved by management outside the period.</p> <p>No further deviations noted.</p> |
| 16.1.2 | <p><i>Reporting information security events</i></p> <p>Information security events are being reported through appropriate management channels as quickly as possible.</p> | <p>We have inspected guidelines for reporting information security incidents and ensured that reporting of incidents has been described.</p> <p>We have inquired about ticket for an event in the period.</p> | <p>We have not received the ticket for the event.</p> <p>No further deviations noted.</p> |
| 16.1.3 | <p><i>Reporting security weaknesses</i></p> <p>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.</p> | <p>We have inspected guidelines for reporting information security incidents and ensured that reporting of incidents has been described.</p> <p>We have inquired about ticket for an event in the period.</p> | <p>We have not received the ticket for the event.</p> <p>No further deviations noted.</p> |
| 16.1.4 | <p><i>Assessment of and decision on information security events</i></p> <p>Information security events are assessed, and it is decided if they are to be classified as information security incidents.</p> | <p>We have inquired about evaluation of the event.</p> | <p>We have not received the evaluation of the event.</p> <p>No further deviations noted.</p> |
| 16.1.5 | <p><i>Response to information security incidents</i></p> <p>Information security incidents are responded to in accordance with the documented procedures.</p> | <p>We have inspected documentation for handling information security incidents during the period.</p> | <p>No deviations noted.</p> |

| No. | twoday A/S' control | We have inspected documentation for that breaches have been evaluated during the period. | 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 inspected documentation for that incidents have been evaluated during the 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 the Business Continuity Plan and ensured that relevant systems are included. | No 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 inquired about evaluation and approval of the disaster recovery plan. | We have been informed that the disaster recovery plan has not been evaluated and approved during the period. No further deviations noted. |
| 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 inquired about test of the disaster recovery plan during the period. | We have been informed that the disaster recovery plan has not been tested during the period. 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 | <p><i>Independent review of information security</i></p> <p>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.</p> | <p>We have observed that independent evaluation of information security has been established.</p> | <p>No deviations noted.</p> |
| 18.2.2 | <p><i>Compliance with security policies and standards</i></p> <p>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.</p> | <p>We have inspected documentation for review of the IT security policy during the period.</p> | <p>No deviations noted.</p> |
| 18.2.3 | <p><i>Technical compliance review</i></p> <p>Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.</p> | <p>We have inspected documentation that the security policy is available for employees.</p> <p>We have inspected documentation for awareness training for employees during the period.</p> | <p>No deviations noted.</p> |

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet med Addo Sign sikker digital underskrift. Underskrivers identitet er fysisk registreret i det elektroniske PDF dokument og vist herunder. Alle tider er angivet i Universaltid (UTC).

Underskrivere

| | |
|---|--|
|   Jesper Drustrup Director / COO 3b4262e0-7ea4-426a-89da-fc3db7c4c385 2023-11-27 14:19:28Z |   Basel Rimon Obari 7a620960-cd2a-41f1-82f4-f2021d544570 2023-11-27 15:05:41Z |
|   Jacob Helly Juell-Hansen Statsautoriseret revisor d606b7c0-b84a-4f0d-b549-9db5ea2e79c4 2023-11-28 11:38:59Z | |

Dokumenter i transaktionen

| | |
|---|---------------------|
| Twoday Addo Sign - ISAE 3402-II - 2023 - Assurance Report.pdf | Nærværende dokument |
|---|---------------------|



Dokumentet er underskrevet digitalt med Addo Sign sikker signeringservice. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument.

Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i PDF dokumentet, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan verificeres dokumentets ægthed

Dokumentet er beskyttet med Adobe CDS certifikat. Når dokumentet åbnes i Adobe Reader, vil det fremstå som være underskrevet med Addo Sign signeringservice.