Twoday Denmark A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 April 2025 to 31 March 2026 in relation to Twoday Denmark A/S' delivery of the Addo Sign service to customers

August 2026

Contents

1. Management's assertion

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

Twoday confirms that:

a) The accompanying description in section 3 fairly presents the IT general controls related to their service delivery throughout the period from 1 April 2025 to 31 March 2026. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to the Addo Sign service were designed and implemented, including:

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

   (ii) Includes relevant details of changes to IT general controls in relation to Addo Sign during the period from 1 April 2025 to 31 March 2026

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 April 2025 to 31 March 2026. The criteria used in making this assertion were that:

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

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

   (iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2025 to 31 March 2026.

Copenhagen, 20 August 2026
Twoday Denmark A/S

Jesper Drustrup
Products Managing Director

2. Independent auditor's assurance report

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 April 2025 to 31 March 2026 in relation to Twoday's Addo Sign service to customers

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

Scope

We have been engaged to report on Twoday's description in section 3 of IT general controls in relation to the Addo Sign service throughout the period from 1 April 2025 to 31 March 2026 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Twoday use the following subservice organisations in the service delivery of Addo Sign to customers:

- team.blue Denmark A/S
- Retarus GmbH
- Compaya A/S

This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Twoday and excludes the control objectives and related controls at subservice organisations.

Some of the control objectives stated in the description in Section 3 can only be achieved if the complementary controls at the user organisations are suitably designed and operationally effective with Twoday's controls. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

Twoday's responsibilities

Twoday is responsible for preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on Twoday's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.
We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design and operating effectiveness of controls. 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 organization and described in section 1.

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

Limitations

Twoday's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the service delivery that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions.
Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 1. In our opinion, in all material respects:

a) The description fairly presents the controls related to the Addo Sign service delivery as designed and implemented throughout the period from 1 April 2025 to 31 March 2026;

b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 April 2025 to 31 March 2026; and

c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved, operated effectively throughout the period 1 April 2025 to 31 March 2026

Description of test of controls

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

Intended users and purpose

The report and the description of tests of controls in Section 4 are intended only for customers who have used Twoday's Addo Sign and who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves in assessing the risks of material misstatements of customers' financial statements.

Copenhagen, 20 August 2026

RSM Denmark
Statsautoriseret Revisionspartnerselskab
Company reg. no. 25 49 21 45

Martin Enderberg Lassen
State Authorised Public Accountant
Mne 40044

Andreas Moos
Head of IT Risk Assurance
CISA | CISM

3. System description

The following is a description of the Addo Sign service by Twoday. The report includes general processes and system setups etcetera with Twoday. 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's general solution for the establishment of a more efficient process for digital signing of documents. The solution is delivered as software as a 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 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 is handled and described in the ISAE 3402 and ISAE 3000 done by the Twoday 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 Group will be included in this ISAE 3402. 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.

The Network area has been excluded from the scope of this audit report and the related control environment. Network management, including network infrastructure, network security, and monitoring, is governed and operated centrally at Twoday group level and is not managed or controlled locally at the country/entity level.

Onboarding of new team members

Onboarding of new team members are handled jointly between the Twoday Group and Addo Sign. The former takes care of onboarding the new team member into the corporate systems (time registration, reimbursement, salary, etc.). 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:

- **Not started:** this is for newly identified items where no action have been taken.
- **Started:** a risk item that is marked as started means that actual work is happening to mitigate the risk.
- **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 user behavioural patterns.
- **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 falls 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 Group under the Products department. The director of the Products department, Jesper Drustrup, is overall responsible for the security policy of Addo Sign. This responsibility includes policies and procedures. All changes to the security policy must be approved by the Products 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 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 logon

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 Gitlab. 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 HubSpot portal with a password-protected access.

Capacity controls

The capacity control of the server environment is conducted by internally by our DevOps and reported to the Addo Sign project members via Slack where necessary.

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'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. Access is granted to the developers as they perform the day-to-day operations of the Addo Sign product as DevOps.

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 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'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 prioritise incidents. The necessary actions can be handled upon the data form, 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

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

Compliance

Independent evaluation of information security

The security function in Twoday continuously performs an audit on all our activities.

Once a year Addo Sign is reviewed by an independent IT auditor, to submit an ISAE 3402 assurance report of compliance controls mentioned in this control description.

Compliance with security policies and security standards

Twoday secure anchoring of the IT security policy by all employees by annually review.

Checking technical compliance

Twoday 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

There are no significant changes in infrastructure or control environment from 1 April 2025 to 31 March 2026.

Complementary user entity controls

Twoday is fully responsible for software and hardware owned by Twoday, as well as the services Twoday performs for customers. However, in any delivery to a customer, there is also aspects for Twoday expects the customer to take responsibility.

These include:

- Any use of the Solution by the Customer's affiliates is subject to these Terms and the Customer is responsible towards twoday for any such use.
- The Solution can be accessed and used by using a username and password.
- The Customer is responsible for storing the username and password securely and confidentially to ensure that the username and password is only used for the Customer's use of the Solution.
- The Customer is responsible for the creation of users and the administration of user rights to the Solution.
- The Customer is responsible for ensuring that documents signed through the Solution are valid and/or enforceable pursuant to applicable Danish or international legislation.
- The Customer is the data controller as regards to the personal data uploaded by the Customer and processed by the Customer in the Solution, whereas twoday is the data processor of such data.

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

Purpose and scope

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation".

Our testing of the design, implementation and operating effectiveness of the controls has included the control objectives and related control activities selected by Management and are listed below.

Our testing has included the control activities deemed necessary to obtain a reasonable level of assurance that the stated control objectives were achieved.

To the extent that our testing identified deviations in the design, implementation, or operating effectiveness of controls, these have been described below.

This report applies the carve-out method, and our testing has not included controls at subservice organizations.

Test procedures

The test procedures performed when determining the design, implementation, or operating effectiveness of controls are described below:

Test procedure	Description of the test procedure
Inquiries	Inquiry of appropriate personnel. Inquiries included how the controls are performed.
Observation	We observed the execution of the control.
Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

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

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			
Nr.	**Twoday's control activity**	**Tests performed by RSM**	**Result of test**
5.1.1	*Policies for information security* A set of policies for information security is de-fined and approved by management, and then published and communicated to employees and relevant exter-nal parties.	Inspected that an Information Security Policy has been established and approved by management. Inspected documentation confirming that the Infor-mation Security Policy has been published and com-municated to relevant parties.	No exceptions 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 ef-fectiveness.	Inspected documentation confirming that the Infor-mation Security Policy has been reviewed and updated.	No exceptions noted.

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	Inspected documentation confirming that an organizational chart for the information security function has been established. Inspected documentation confirming that roles and responsibilities within the information security function have been defined.	No exceptions noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.	Inspected that a procedure exists to segregate conflicting duties and responsibilities.	No exceptions noted.

A.6.2 Mobile devices and teleworking

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
6.2.1	*Mobile device policy* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	Inspiceret, at der foreligger en politik for anvendelse af mobilt udstyr.	No exceptions noted.
6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	Inspected that a policy for secure remote working arrangements has been established. Inspected documentation confirming that multi-factor authentication (MFA) was implemented and enabled for employees working remotely. Inspected documentation confirming that virtual private networks (VPN) are used to ensure secure communication for employees working remotely.	No exceptions noted.

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected, by sample test, that signed employment contracts define the employee's and the organization's information security responsibilities.	No exceptions noted.

A.7.2 During employment

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation confirming that guidelines have been established requiring relevant parties to maintain information security in accordance with the organization's policies and procedures.	No exceptions noted.
7.2.2	*Information security awareness education and training* All 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.	Inspected documentation confirming that an information security awareness program has been established. Inspected documentation confirming that the organization's employees have completed information security training. Inspected documentation confirming that the organization has established a control to follow up with employees who have not completed information security awareness training.	No exceptions noted.

A.7.2 During employment

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation confirming that a disciplinary process has been established and communicated to employees. Inspected, by sample test, that signed employment contracts include the disciplinary process.	No exceptions 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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation confirming that information security responsibilities and obligations applicable after termination or change of employment have been defined. Inspected, by sample test, that terminated employees were informed that information security responsibilities and obligations remain applicable after termination of employment.	No exceptions noted.

A.8.1 Responsibility for assets

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation confirming that an asset inventory has been developed and maintained.	No exceptions noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	Inspected documentation confirming that asset owners have been assigned.	No exceptions 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.	Inspected documentation confirming that a procedure for acceptable use of information and assets has been established. Inspected documentation confirming that rules for acceptable use of information and assets have been implemented.	No exceptions 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.	Inspected documentation confirming that a procedure for the return of assets has been established. Inspected, by sample test, that employees returned organizational assets upon termination of employment.	No exceptions noted.

A.9.1 Business requirements of access control

Control objective: To limit access to information and information processing facilities

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	Inspected documentation confirming that an Access Control Policy has been established. Inspected documentation confirming that the policy has been updated.	No exceptions noted.

A.9.2 User access management

Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation confirming that formal procedures for granting and revoking user access rights have been established. Inspected, by sample test, that new user registrations were approved. Inspected, by sample test, that user accounts for terminated employees were deactivated.	No exceptions noted.
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.	Inspected documentation confirming that a user administration procedure has been established. Inspected, by sample test, that user access assignments were approved. Inspected, by sample test, that user access for terminated employees was removed.	No exceptions noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	Inspected documentation confirming that a procedure for privileged access rights has been established.	No exceptions noted.

A.9.2 User access management Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services			
Nr.	**Twoday's control activity**	**Tests performed by RSM**	**Result of test**
		Inspected documentation confirming that privileged access is restricted and granted based on business need.	
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	Inspected documentation confirming that a Password Policy has been established. Inspected documentation confirming that implemented password parameters comply with the Password Policy.	No exceptions noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals	Inspected that a procedure for reviewing access rights has been established. Inspected documentation confirming that access rights reviews have been performed.	No exceptions 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.	Inspected documentation confirming that a user administration procedure has been established. Inspected, by sample test, that user access for terminated employees was removed.	No exceptions noted.

A.9.3 User responsibilities

Control objective: To make users accountable for safeguarding their authentication information

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
9.3.1	*Use of secret authentication information* Users are required to follow the organisations' s practices in the use of secret authentication information.	Inspected documentation confirming that a Password Policy has been established. Inspected documentation confirming that implemented password parameters comply with the Password Policy.	No exceptions noted.

A.9.4 System and application access control

Control objective: To prevent unauthorised access to systems and applications

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
9.4.2	*Secure logon procedures* Access to systems and applications is controlled by procedure for secure logon.	Inspected documentation confirming that a secure logon procedure has been established. Inspected documentation confirming that multi-factor authentication (MFA) has been implemented.	No exceptions noted.
9.4.5	*Access control to program source code* Access to program source code has been restricted.	Inspected documentation confirming that a procedure for restricting access to source code has been established. Inspected documentation confirming that access to source code is restricted to employees with a business need.	No exceptions noted.

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			
Nr.	**Twoday's control activity**	**Tests performed by RSM**	**Result of test**
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.	Inspected documentation confirming that a policy for the use of encryption has been established.	No exceptions 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.	Inspected documentation showing that a policy exists for the administration of encryption keys. Inspected documentation showing that encryption certificates are active.	No exceptions noted.

A.11.1 Secure areas Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities			
Nr.	**Twoday's control activity**	**Tests performed by RSM**	**Result of test**
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.	Inspected documentation showing that policies and procedures for physical security exist. Observed that perimeter protection has been established to protect information and information processing facilities.	No exceptions noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Inspected documentation showing that policies and procedures for physical security exist. Observed that only authorized personnel can gain access to secure areas by using access cards.	No exceptions noted.
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	Inspected documentation showing that policies and procedures for physical security exist. Inspected access points and entrances to determine whether personal access cards had to be used to gain access to the office. Inspected documentation showing that alarms were installed on physical access control and that these were activated.	No exceptions noted.

A.11.2 Equipment Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations			
Nr.	**Twoday's control activity**	**Tests performed by RSM**	**Result of test**
11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	Inspected the procedure for protection of portable media and unattended equipment. Inspected the clean desk and locked screen policy.	No exceptions 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.	Inspected the procedure for protection of portable media and unattended equipment. Inspected the clean desk and locked screen policy.	No exceptions noted.

A.12.1 Operational procedures and responsibilities Control objective: To ensure correct and secure operation of information processing facilities			
Nr.	**Twoday's control activity**	**Tests performed by RSM**	**Result of test**
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been con-trolled.	Inspected documentation showing that a change management procedure had been established. Inspected, by sample test, that changes were approved before being put into production. Inspected, by sample test, that changes were tested before being put into production.	No exceptions noted.
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.	Inspected documentation showing that a procedure for monitoring resources and capacity adjustments had been established. Inspected documentation showing that information processing resources are monitored. Inspected documentation showing that monitoring had been implemented to identify problems.	No exceptions noted.
12.1.4	*Separation of development-, test- and operations facilities.* Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.	Inspected documentation showing that development, test, and production environments were segregated.	No exceptions noted.

A.12.2 Protection from malware

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	Inspected documentation showing that a procedure for protection against malware had been established. Inspected, by sample test, that anti-malware was installed on the servers. Inspected, by sample test, that anti-malware was installed on laptops. Inspected, by sample test, that regular user awareness training is conducted.	No exceptions noted.

A.12.4 Logging and monitoring

Control objective: To record events and generate evidence

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	Inspected documentation showing that a procedure for log management had been established. Inspected documentation showing that logs are configured in accordance with the procedure, including, as a minimum: - User ID - System activities - Dates, times, and event details.	No exceptions noted.
12.4.4	*Clock synchronization* The clocks of all relevant information pro-cessing systems within an organisation or security domain have been synchronised to a single reference time source.	Inspected documentation showing that clocks used by the organization for information processing and supporting information processing systems were synchronized with approved time sources.	No exceptions noted.

A.12.6 Technical vulnerability management

Control objective: To prevent exploitation of technical vulnerabilities

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation showing that a procedure for managing technical vulnerabilities had been established. Inspected documentation showing that vulnerability scans are performed regularly. Inspected documentation showing that all deviations or weaknesses had been responded to.	No exceptions noted.

A.15.2 Supplier service delivery management

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	Inspected that procedures have been defined for monitoring and periodic assessment of suppliers' deliveries and security obligations. Inspected documentation that reviews/monitoring of relevant suppliers had been carried out.	No exceptions 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.	Inspected that there is a procedure for handling supplier services.	No exceptions noted. We have noted that there have been no relevant changes to third-party services and supplier agreements.

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	Inspected documentation that a procedure for managing information security incidents had been established. Inspected documentation that roles and responsibilities related to the management of information security incidents had been defined and made available to relevant employees.	No exceptions noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	Inspected documentation that a procedure for reporting information security incidents had been established. Inquired whether any information security breaches had occurred.	No exceptions noted. We have noted that there have been no registered information security breaches during the audit period.
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.	Inspected that there are guidelines for reporting information security weaknesses. Inquired whether any information security weaknesses had occurred.	No exceptions noted. We have noted that there have been no registered information security breaches during the audit period.
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.	Inspected documentation that a procedure for assessing and deciding on information security incidents had been established. Inquired whether any information security breaches had occurred.	No exceptions noted. We have noted that there have been no registered information security breaches during the audit period.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	Inspected documentation for an established procedure for handling information security incidents. Inquired whether any information security breaches had occurred.	No exceptions noted. We have noted that there have been no registered information security breaches during the audit period.

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation that a procedure for learning from information security incidents had been established. Inquired whether any information security breaches had occurred.	No exceptions noted. We have noted that there have been no registered information security breaches during the audit period.

A.17.1 Information security continuity

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation that the organization's contingency plans had been prepared and approved by management. Inspected documentation that contingency plans had been made available to relevant employees.	No exceptions noted.

A.17.1 Information security continuity

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation that contingency plans were up to date.	No exceptions 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.	Inspected documentation that contingency plans had been tested.	No exceptions noted.

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

Nr.	Twoday's control activity	Tests performed by RSM	Result of test
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.	Inspected documentation that an independent review of the organization's information security had been carried out, including the implementation and operation in accordance with policies and procedures.	No exceptions noted.

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
Acting Managing Director, Products
3b4262e0-7ea4-426a-89da-fc3db7c4c385 *2026-08-20 13:10:18Z*

Andreas Moos
Head of IT Risk Assurance, RSM Danmark
0303be40-d0bf-4b67-8a20-e59d09e0be9c *2026-08-21 06:39:38Z*

Martin Enderberg Lassen
Statsautoriseret Revisor
468a1249-a838-4bbe-a1c8-63a6f30f262d *2026-08-21 07:25:26Z*

Dokumenter i transaktionen

twoday_AddoSign_ISAE3402_Type2_Aug_2026_assurance report Final.pdf *SHA256:*
319765280af11d1723f20b99bafa8b39af05a3b1046cdd4a43b5cf8ab9ffc594