

MyDesk ApS

**Independent service auditor's ISAE 3402 assurance report
on IT general controls during the period from 1 August 2025
to 31 July 2026 in relation to MyDesk ApS' SaaS solution to
customers**

October 2026

Contents

1. Management's assertion	3
2. Independent auditor's assurance report	4
3. System description	6
4. Control objectives, control activity, tests and test results	9

1. Management's assertion

The accompanying description has been prepared by MyDesk ApS (MyDesk) for customers who have used the SaaS solution 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 obtaining an understanding of customers' information systems relevant to financial reporting.

MyDesk 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 August 2025 to 31 July 2026. The criteria used in making this statement were that the accompanying description:
 - (i) Presents how IT general controls in relation to the SaaS solution 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 the service delivery
 - (ii) Includes relevant details of changes to IT general controls in relation to the service delivery during the period from 1 August 2025 to 31 July 2026
 - (iii) Does not omit or distort information relevant to the scope of IT general controls in relation to the service delivery 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 IT general controls in relation to the service delivery 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 August 2025 to 31 July 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 August 2025 to 31 July 2026.

Taastrup, 6 October 2026

MyDesk ApS

Jesper Bo Larsen
CEO

2. Independent auditor's assurance report

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 August 2025 to 31 July 2026 in relation to MyDesk's delivery of SaaS solution to customers

To: MyDesk ApS (MyDesk), its customers and their auditors

Scope

We have been engaged to report on MyDesk's description in section 3 of IT general controls in relation to the SaaS solution throughout the period from 1 August 2025 to 31 July 2026 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

MyDesk use the following subservice organisations in the service delivery to customers:

- Microsoft Azure (Microsoft)

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

Some of the control objectives stated in the description in Section 4 can only be achieved if the complementary controls at the user organisations are suitably designed and operationally effective with MyDesk's controls. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

MyDesk's responsibilities

MyDesk 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 MyDesk'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

MyDesk'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 SaaS solution as designed and implemented throughout the period from 1 August 2025 to 31 July 2026;
- b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 August 2025 to 31 July 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 August 2025 to 31 July 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 MyDesk's SaaS solution 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, 6 October 2026

RSM Denmark

Statsautoriseret Revisionspartnerselskab
CVR-nr. 25 49 21 45

Martin Enderberg Lassen
State Authorised Public Accountant
mne40044

Alexander Petersen
Head of IT Risk & Compliance

3. System description

3.1. Introduction

MyDesk ApS delivers and implements an application for managing flexible workplaces, including desk reservations and meeting room bookings, for a range of companies.

Using the MyDesk application, employees can book or register for the following:

- Desks
- Meeting rooms
- Parking spaces
- Canteen lunches
- Meeting catering
- Visitors

The solution is available through the following channels:

- Web browser
- Mobile apps for Android and iOS
- Outlook on the web and desktop
- Microsoft Teams

3.2. Description of services

The primary services of MyDesk are as follows:

- Delivery and operation of the MyDesk application based on Microsoft technology, hosted in Microsoft Azure
- Preparation and maintenance of customers' floor plans in 3D
- Ongoing 2nd level customer support
- Training and assistance with internal communication for our customers during the rollout of the MyDesk application.

The MyDesk application is hosted in a Microsoft data center in Ireland with a failover to the Netherlands.

Support and development is based in Denmark and Danish-speaking. Support is available from 9-16 unless extended support is purchased. We currently support approximately 10,000 Danish employees and companies.

Most of our customers handle their own 1st level support, while MyDesk manages second level support.

3.3. Organising

MyDesk is currently led by two directors, Henrik Jøhnk Kristensen and Jesper Bo Larsen, in collaboration and is presently located in Høje Taastrup.

There have been no significant changes to procedures and controls in the period from 1 August 2025 to 31 July 2026.

3.4. Control environment

MyDesk has formalised procedures for version control and management of deployments. General policies and procedures are described in the document "Guidelines in the organization - MyDesk".

Control objectives and activities are detailed in section 4.

The responsibility for security policy, operational routines, and the description of business processes lies with the management. It is the management that communicates externally with, for example, the press. The responsibility for the dissemination of business processes and internal routines lies with the management. In the event of updates/revisions, it is the management's responsibility to communicate these.

3.5. Risk management

The management has the overall responsibility for MyDesk's security work.

MyDesk continuously uses an external partner, Arrow ECS, ensuring our installation is carried out and maintained following best practices in terms of technology and security.

In MyDesk the internal administrative security function is performed by the technical manager – Henrik Jøhnk Kristensen. The function ensures the implementation and updating of security and quality procedures, manages the primary contact with auditors, ensures the execution of self-controls, ensures ongoing maintenance of risk assessment and ensures that a contingency plan exists and is continuously updated.

It is the responsibility of each employee to continually follow the professional development within their area and keep their educational level up to date. The employee is entitled and obligated to relevant further education, which is agreed upon with the immediate superior. MyDesk covers all costs for this education. Once a year, follow-up on education is conducted in performance review meetings – for individual employees a yearly plan is made. This is included in the minutes from the performance review meetings, where other personal matters are also described.

MyDesk's general policies and business procedures are described in the document "Guidelines in the organization - MyDesk".

The responsibility for security policy, contingency plans, operational routines and description of business processes lies with the management. It is the management that communicates externally with, for example, the press. The responsibility for the dissemination of business processes and internal routines lies with the management. In the event of updates/revisions, it is the management's responsibility to communicate these.

It is up to the customer to claim specific security routines or technical installations if best practices in terms of technology and security, according to MyDesk's standard, do not meet this.

It is not possible to physically access MyDesk's data centre as it is hosted in Microsoft Azure Cloud and employees can only log in via two-factor authentication.

3.6. Information and communication

It is the individual manager's responsibility to communicate internally at MyDesk. Similarly, the management is responsible for communication with customers and the press.

Reports are prepared by each unit and approved by the management before being sent to the customer.

3.7. Monitoring

Management is responsible for monitoring security breaches and addressing them. Additionally, management initiates the remediation of any security issues. Employees are responsible for immediately reporting security breaches or suspected breaches to management.

3.8. Control activities

MyDesk's information policy is available to employees on the intranet. All users are logged in AD. These logs are reviewed when there is reasonable suspicion, and all AD users and their rights are reviewed at least twice a year.

MyDesk only uses standard systems.

3.9. Complementary controls at the customers

The customer is responsible for ensuring that access to MyDesk functions as intended, that the correct employees have admin rights, and that consent is provided according to MyDesk's instructions. MyDesk itself does not have access to the customer's information and cannot verify the above.

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 operating effectiveness testing included the control activities deemed necessary to obtain reasonable 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. Microsoft is a service organisation providing online services (Microsoft Azure) to MyDesk. Our testing did not extend to controls of Microsoft.

Test procedures

The test procedures performed when determining the design, implementation and 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 Organisational controls

Control objective: The organization maintains governance structures, policies, procedures, and oversight mechanisms to direct, manage, and monitor information security in alignment with strategic, operational, legal, regulatory, and contractual requirements

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
5.1	<i>Policies for information security</i> Information security policy and topic-specific policies should be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Inspected documentation that the information security policy was approved by management, published, and communicated to employees. Inspected documentation that the information security policy was updated.	No exceptions noted.
5.2	<i>Information security roles and responsibilities</i> Information security roles and responsibilities should be defined and allocated according to the organisation needs.	Inspected documentation of an organisation chart showing the information security organisation. Inspected documentation of the description of roles and responsibilities within the information security organisation.	No exceptions noted.
5.3	<i>Segregation of duties</i> Conflicting duties and conflicting areas of responsibility should be segregated.	Inspected documentation of organisation charts showing that segregation of duties was established on an organisational level.	No exceptions noted.
5.4	<i>Management responsibilities</i> Management should require all personnel to apply information security in accordance with the established information security policy, topic-specific policies, and procedures of the organisation.	Inspected documentation that the management, in employment contracts, has required personnel must comply with information security policies and procedures. Inspected, by sample test, that the requirements for compliance with information security measures was included in an employee's employment contract.	No exceptions noted.

A.5 Organisational controls

Control objective: The organization maintains governance structures, policies, procedures, and oversight mechanisms to direct, manage, and monitor information security in alignment with strategic, operational, legal, regulatory, and contractual requirements

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
5.16	<i>Identity management</i> The full life cycle of identities should be managed.	Inspected, by sample test, that identities were assigned unique user IDs that enable the traceability of actions performed. Inspected, by sample test, that assignment of user access rights were granted based on the job function and an approval from the immediate superior. Inspected, by sample test, that removal of user access rights were performed in a timely manner upon termination.	No exceptions noted.
5.17	<i>Authentication information</i> Allocation and management of authentication information should be controlled by a management process, including advising personnel on the appropriate handling of authentication information.	Inspected documentation that a password management procedure was designed. Inspected documentation that the password configuration settings were set in accordance with the procedure.	No exceptions noted.
5.18	<i>Access rights</i> Access rights to information and other associated assets should be provisioned, reviewed, modified, and removed in accordance with the organisation's topic-specific policy on and rules for access control.	Inspected, by sample test, that assignment of user access rights were granted based on the job function and an approval from the immediate superior. Inspected, by sample test, that removal of user access rights were performed in a timely manner upon termination. Inspected documentation that access rights had been reviewed on a regular basis and at least annually.	No exceptions noted.

A.5 Organisational controls

Control objective: The organization maintains governance structures, policies, procedures, and oversight mechanisms to direct, manage, and monitor information security in alignment with strategic, operational, legal, regulatory, and contractual requirements

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
5.19	<i>Information security in supplier relationships</i> Processes and procedures should be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Inquired with Management about the procedures/control activities performed. Inspected documentation that the procedure for managing supplier relationships and service agreements, contains requirements to mitigate risks connected with suppliers' access to assets.	No exceptions noted.
5.20	<i>Addressing information security within supplier agreements</i> Relevant information security requirements should be established and agreed with each supplier based on the type of supplier relationship.	Inquired with Management about the procedures/control activities performed. Inspected, by sample test, that supplier agreements contain relevant information security requirements.	No exceptions noted.
5.22	<i>Monitoring, review and change management of supplier services</i> The organisation should regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Inspected documentation that a procedure for supplier management has been designed. Inspected, by sample test, that monitoring activities, covering outsourced supplier services, was performed for suppliers.	No exceptions noted.
5.29	<i>Information security during disruption</i> The organisation should plan how to maintain information security at an appropriate level during disruption.	Inspected documentation that contingency plans were designed and approved by management. Inspected documentation that the contingency plans were made available to relevant employees. Inspected and verified that the plan was reviewed and approved by Management during the period.	No exceptions noted.

A.5 Organisational controls

Control objective: The organization maintains governance structures, policies, procedures, and oversight mechanisms to direct, manage, and monitor information security in alignment with strategic, operational, legal, regulatory, and contractual requirements

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
5.30	<i>ICT readiness for business continuity</i> ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.	Inspected the disaster recovery plan and verified that the disaster recovery plan is updated at least annually. Inspected documentation that the contingency plans were tested.	No exceptions noted.

A.7 Physical controls

Control objective: The organization protects physical environments, facilities, equipment, and information assets against unauthorized physical access, damage, theft, loss, and environmental threats

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
7.1	<i>Physical security perimeters</i> Security perimeters should be defined and used to protect areas that contain information and other associated assets.	Inspected documentation of the procedure for physical protection of facilities and security perimeters. Inspected documentation of relevant locations and their security perimeters to establish whether security measures were implemented to prevent unauthorised access.	No exceptions noted.

A.8 Technological controls

Control objective: The organization designs, implements, and operates technical security controls to protect systems, applications, networks, and information assets against unauthorized access, misuse, alteration, disclosure, or disruption

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
8.2	<i>Privileged access rights</i> The allocation and use of privileged access rights should be restricted and managed.	Inspected documentation that a procedure for administration of privileged access rights was designed. Inspected, by sample test, that assignment of privileged access rights was granted based on an approval from the immediate superior. Inspected, by sample test, that privileged access rights were restricted to a work-related need.	No exceptions noted.
8.5	<i>Secure authentication</i> Secure authentication technologies and procedures should be implemented based on information access restrictions and the topic-specific policy on access control.	Inspected documentation that a password management procedure was designed. Inspected documentation that the password configuration settings were set in accordance with the defined procedure. Inspected documentation that multi-factor authentication were installed and enabled.	No exceptions noted.
8.7	<i>Protection against malware</i> Protection against malware should be implemented and supported by appropriate user awareness.	Inspected documentation that a procedure for protection against malware was designed. Inspected, by sample test, that anti-malware was installed on servers. Inspected, by sample test, that anti-malware was installed on laptops.	No exceptions noted.

A.8 Technological controls

Control objective: The organization designs, implements, and operates technical security controls to protect systems, applications, networks, and information assets against unauthorized access, misuse, alteration, disclosure, or disruption

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
8.13	<i>Information backup</i> Backup copies of information, software and systems should be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	Inspected documentation that a procedure for backup of data was designed. Inspected, by sample test, that backup copies of were made continuously in accordance with the procedure. Inspected, by sample test, that daily backup reports were received from the backup system specifying whether the backup was successfully completed. Inspected, by sample test, that failed or erroneous backup jobs were identified and corrected. Inspected documentation that regular tests were performed of backup data to verify that the data can be re-stored from backup files.	No exceptions noted.
8.15	<i>Logging</i> Logs that record activities, exceptions, faults and other relevant events should be produced, stored, protected and analysed.	Inspected documentation that a procedure for log management was designed. Inspected documentation that logs were configured in accordance with the procedure including, as a minimum, the caption of: - user IDs - system activities - dates, times and details of events Inspected documentation that logs collected were protected against manipulation or deletion.	No exceptions noted.
8.16	<i>Monitoring activities</i> Networks, systems and applications should be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	Inspected documentation that a procedure for monitoring activities of log information was designed. Inspected documentation that log information was monitored in accordance with the procedure. Inspected, by sample test, that adequate follow-up on monitoring alerts and logs from critical systems was performed during the period.	No exceptions noted.

A.8 Technological controls

Control objective: The organization designs, implements, and operates technical security controls to protect systems, applications, networks, and information assets against unauthorized access, misuse, alteration, disclosure, or disruption

Nr.	MyDesk control activity	Tests performed by RSM	Result of test
8.19	<i>Installation of software on operational systems</i> Procedures and measures should be implemented to securely manage software installation on operational systems.	Inspected documentation that a procedure for installation of software on operational systems was designed. Inspected that server operating systems were patched in accordance with the procedure.	No exceptions noted.
8.31	<i>Separation of development, test and production environments</i> Development, testing and production environments should be separated and secured.	Inspected documentation that development, testing and production environments were separated.	No exceptions noted.
8.32	<i>Change management</i> Changes to information processing facilities and information systems should be subject to change management procedures.	Inspected documentation that a change management procedure was designed. Inspected, by sample test, that key stakeholders have approved changes prior to release into production. Inspected, by sample test, that changes were tested based on established criteria prior to release into production.	No exceptions noted.

PENNEO

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

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

Jesper Bo Larsen

Underskriver

Serienummer: 9f433cc2-68e8-4de8-be4d-017108fe6c7a

IP: 2.109.xxx.xxx

2026-10-06 06:23:10 UTC



Alexander Petersen

RSM DANMARK STATSATORISERET

REVISIONSPARTNERSELSKAB CVR: 25492145

Underskriver

Serienummer: 7d1d699a-1afd-4a8a-9365-3d74a085135e

IP: 194.19.xxx.xxx

2026-10-06 06:26:19 UTC



Martin Enderberg Lassen

RSM DANMARK STATSATORISERET

REVISIONSPARTNERSELSKAB CVR: 25492145

Statsautoriseret revisor

Serienummer: 95e5c5c1-e970-4707-b7e7-906938abe592

IP: 194.19.xxx.xxx

2026-10-06 06:38:09 UTC



Dette dokument er underskrevet digitalt via **Penneo.com**. De underskrevne data er valideret vha. den matematiske hashværdi af det originale dokument. Alle kryptografiske beviser er indlejret i denne PDF for validering i fremtiden.

Dette dokument er forseglet med et kvalificeret elektronisk segl. For mere information om Penneos kvalificerede tillidstjenester, se <https://eutl.penneo.com>.

Sådan kan du verificere, at dokumentet er originalt

Når du åbner dokumentet i Adobe Reader, kan du se, at det er certificeret af **Penneo A/S**. Dette beviser, at indholdet af dokumentet er uændret siden underskriftstidspunktet. Bevis for de individuelle underskrivers digitale underskrifter er vedhæftet dokumentet.

Du kan verificere de kryptografiske beviser vha. Penneos validator, <https://penneo.com/validator>, eller andre valideringstjenester for digitale underskrifter.