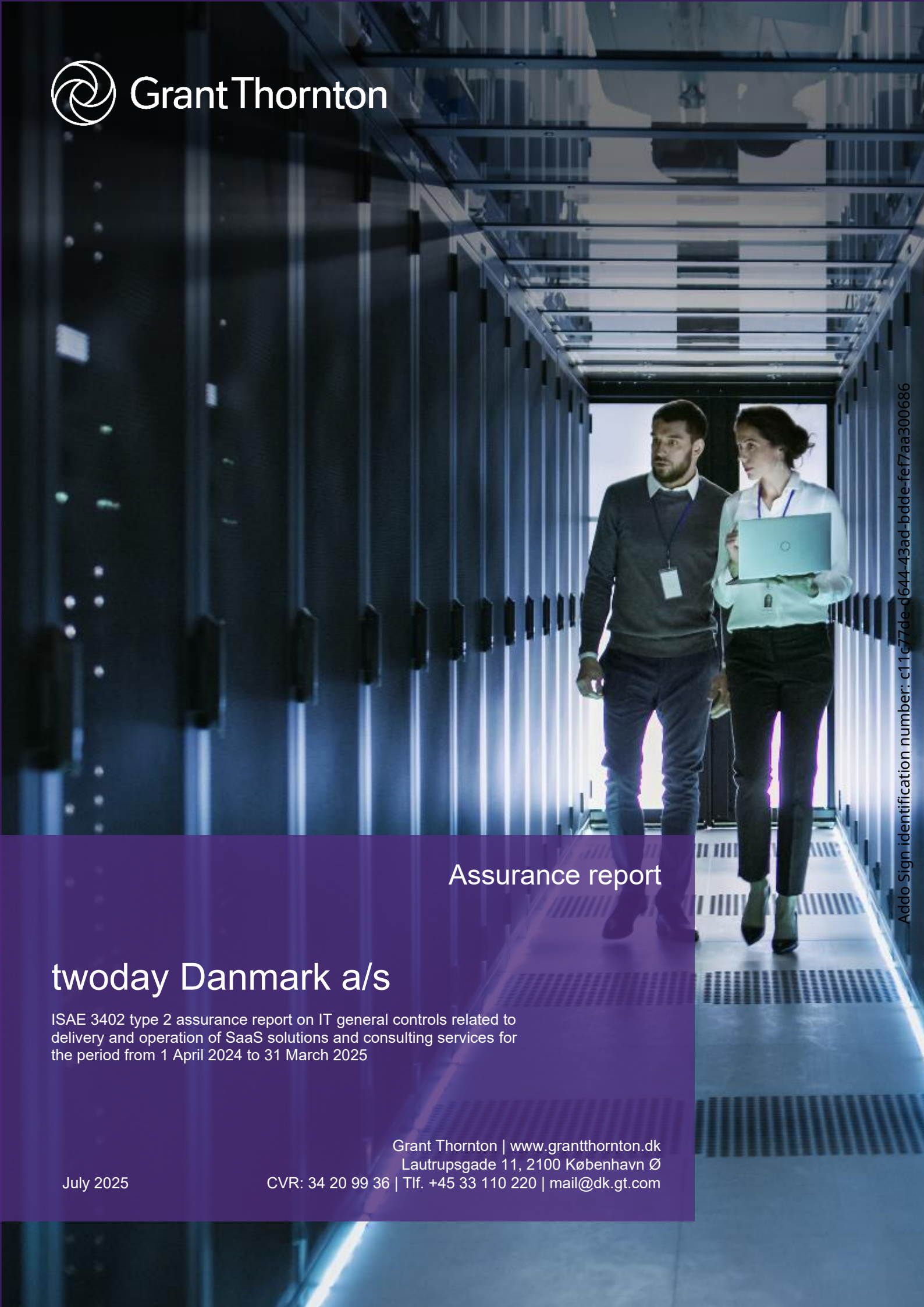

Assurance report

twoday Danmark a/s

ISAE 3402 type 2 assurance report on IT general controls related to delivery and operation of SaaS solutions and consulting services for the period from 1 April 2024 to 31 March 2025

Grant Thornton | www.grantthornton.dk
Lautrupsgade 11, 2100 København Ø
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

July 2025

Table of contents

Section 1: twoday Danmark a/s' statement

The accompanying description has been prepared for customers who have used twoday Danmark a/s' SaaS solutions and consulting services, 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 Danmark a/s is using the subservice organisations Itm8 A/S, team.blue Denmark A/S, Twilio Inc, Cloud Factory A/S, Compaya A/S and Microsoft Corporation Inc. This assurance report is prepared in accordance with the carve-out method and twoday Danmark a/s' description does not include control objectives and controls within Itm8 A/S, team.blue Denmark A/S, Twilio Inc, Cloud Factory A/S, Compaya A/S and Microsoft Corporation Inc. Certain control objectives in the description can only be achieved, if the subservice organisations' controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subservice organisations.

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

twoday Danmark a/s confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to twoday Danmark a/s' SaaS solutions and consulting services processing of customer transactions throughout the period from 1 April 2024 to 31 March 2025. 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
      - Services provided by subservice organisations, including whether they are included according to the inclusive method or the carve-out method
      - Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

   (ii) Contains relevant information about changes in the IT general controls, performed during the period from 1 April 2024 to 31 March 2025

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

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period 1 April 2024 to 31 March 2025 if relevant controls with the subservice organisation were operationally effective and the customers have performed the complementary user entity controls, assumed in the design of twoday Danmark a/s controls during the entire period from 1 April 2024 to 31 March 2025.

The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2024 to 31 March 2025

Copenhagen, 4 July 2025
twoday Danmark a/s

Lars Engell Berthelsen
Chief Executive Officer

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

To twoday Danmark a/s, their customers and their auditors.

Scope

We have been engaged to report on twoday Danmark a/s' description in Section 3 of its system for delivery of twoday Danmark a/s' SaaS solutions and consulting services throughout the period from 1 April 2024 to 31 March 2025 and about the design and operational effectiveness of controls related to the control objectives stated in the description.

twoday Danmark a/s is using subservice organisations Itm8 A/S, team.blue Denmark A/S, Twilio Inc, Cloud Factory A/S, Compaya A/S and Microsoft Corporation Inc. This assurance report is prepared in accordance with the carve-out method and twoday Danmark a/s' description does not include control objectives and controls within Itm8 A/S, team.blue Denmark A/S, Twilio Inc, Cloud Factory A/S, Compaya A/S and Microsoft Corporation Inc. Certain control objectives in the description can only be achieved if the subservice organisations' controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subservice organisations.

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

twoday Danmark a/s' responsibility

twoday Danmark a/s is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, twoday Danmark a/s is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on twoday Danmark a/s' description (Section 3) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service

organisation's description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation in Section 3.

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

Limitations of controls at a service organisation

twoday Danmark 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 Danmark a/s' statement in Section 1 and based on this, it is our opinion that:

(a) the description fairly presents how the IT general controls in relation to twoday Danmark a/s' SaaS solutions and consulting services were designed and implemented throughout the period from 1 April 2024 to 31 March 2025.

(b) the controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 April 2024 to 31 March 2025 in all material respects, and

(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, operated effectively throughout the period from 1 April 2024 to 31 March 2025.

Description of tests of controls

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

Intended users and purpose

This assurance report is intended only for customers who have used twoday Danmark a/s and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 4 July 2025

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Partner, CISA, CISM

Section 3: Description of twoday Danmark a/s' services related to delivery and operation of SaaS solutions and consulting services, and related IT general controls

The following describes twoday Danmark a/s' services delivered to customers which are governed by the IT general controls in scope for this statement. The statement covers general processes and systems configurations, etc., at twoday Danmark a/s. Specific processes and system configurations, etc., are not covered by this statement and will be subject to specific statements made upon order by the customer. Controls in applications are not in scope for this statement.

Introduction

The following describes the general IT-controls related to twoday Danmark a/s' services delivered to customers.

Use of suppliers

twoday Danmark a/s uses significant suppliers in relation to the delivery of SaaS and consulting services. The significant suppliers are listed in Section 1 of this assurance report.

The company and our performance

twoday Danmark a/s delivers fit-for-purpose software and systems to the public sector and private companies as well as twoday products as a service (SaaS) and custom-made solutions to the public sector and large private regulated companies. To customers with needs beyond the capabilities of standard products, we deliver tailor-made solutions. Our mission is to expand our position as a preferred partner and supplier of software solutions enabling and supporting the continuous development and enhancement of the digital society and e-governance in the Nordic countries. Since 2000, the Nordic governments have focused on building a digital society and have seen the digitalisation of the public sector as a cornerstone in preserving our welfare society during times of demographic shifts and increased competition from developing countries. This requires continuously becoming more effective, and digital services to the public sector is a key element.

Making the Nordics digital

We constantly work on making the Nordics digital, helping both public and private companies design, develop, modernise, and maintain software. We deliver both custom-made and commercial solutions. Together with our customers, we deliver increased productivity and growth in the Nordics for the benefit of us all. In close collaboration with the customer, we develop end-to-end business solutions and self-service solutions that help customers improve productivity through digitalisation, automation, and integration of business processes. Additionally, we provide services for maintaining, supporting, and enhancing the solutions as part of the entire lifecycle, thereby keeping the solutions updated and effective over time.

High level of rules and regulations

twoday Danmark a/s handles some of the largest IT contracts in the public sector, many of which are long-term contracts (4-6 years) and include mission-critical solutions with a high level of rules and regulations. Therefore, we establish long-term partnerships with our customers and invest in building value-adding domain knowledge to secure our customers' satisfaction. The engagement with several of our customers has lasted more than 25 years.

We are constantly improving our compliance and governance setup as our business expands into other regulated sectors, and regulatory and compliance requirements change to keep up with development in technology and political landscape.

Product and services compliance

Both consulting services and products are delivered to customers after entering a formal written agreement between the customer and twoday Danmark a/s. The agreements are by default based on twoday Danmark a/s' templates/standard contracts adjusted according to twoday Danmark a/s' delivered services. In cases where the agreement is based on the customer's template/standard contract, twoday Danmark a/s ensures that services delivered are adjusted to fit the agreement's terms and conditions, including public tenders or purchases under SKI's frame agreements. In the event twoday Danmark a/s is processing personal data on behalf of the customer (i.e., twoday Danmark a/s enters the role of data processor), a data processing agreement (DPA) is created between the parties as the basis for the data processing activities. DPAs are by default established based on twoday Danmark a/s' templates but can also be based on other compliant templates.

Information security policy

twoday Danmark a/s' information security management system (ISMS) is based on the twoday group's information security baseline, which is based on ISO 27001. The ISMS is the foundation for the organisation's information security standards and information security management, including selection/scoping, implementation, and management of controls based on the organization's information security risk profile and appetite. The information security policy is reviewed annually and approved by executive management.

Risk management

Handling of risks
twoday Danmark a/s continuously monitors the development of risks and opportunities to ensure that twoday Danmark a/s' information security work addresses the most significant risks and opportunities, enabling us to ensure that we achieve the intended results, prevent or minimise undesirable effects, and achieve continuous improvement.

We plan:

- actions to address these risks and opportunities and how:
- the actions are integrated and implemented in the information security-related management system processes; and
- the result-related effectiveness of these actions is evaluated.

Based on this model, a risk analysis for threats against business-critical assets is prepared. The risk analysis is prepared by the relevant system owner. If the risk analysis shows a high probability or a significant consequence of a given threat, an action plan for the incident is made, and preventive measures can also be initiated. The risk analysis for each asset is reviewed annually, and the overall risk analysis is approved annually by management.

Organisation of information security

Internal organisation
twoday and thus twoday Danmark a/s is part of the joint forum for information security that has the responsibility to ensure that the information security policy is visible, coordinated, and implemented. Security-responsible system owners for business-critical systems have the responsibility and authority to ensure adequate protection. twoday Danmark a/s collaborates with data security supervisory authorities when they contact twoday Danmark a/s or if twoday Danmark a/s experiences an incident where the supervisory authorities need to be involved. A crisis management plan is prepared for scenarios where contact with the authorities is necessary.

The organisation's IT security officers must keep themselves informed about changes in security threats within relevant technologies, including to:

- Improve knowledge of best practices and stay up to date with relevant security information
- Ensure a broad and updated understanding of information security
- Receive early warnings about alarms, alerts, and patches concerning attacks and vulnerabilities
- Create appropriate contact points for handling information security breaches.

Mobile equipment and remote workstations

twoday Danmark a/s uses mobile equipment and remote workstations in certain contexts for task resolution. Therefore, twoday Danmark a/s has established a set of rules and procedures and implemented several measures to minimise the particular security risks that mobile equipment and remote workstations may pose.

Personnel security

twoday Danmark a/s' employees are our most important asset, both generally and concerning information security. Our skilled employees ensure a high level of information security, but employees can also pose a risk of security breaches, intentional or unintentional. It is therefore essential that our employees are selected and trained to ensure a high degree of information security. Rules and procedures have been established for handling personnel security before, during, and after employment. Permanent and temporary employees with access to twoday Danmark a/s' IT systems must read the information security policy upon joining. It is management's responsibility to ensure that all employees:

- Are sufficiently informed about their roles and responsibilities in connection with security
- Are made aware of the necessary guidelines to comply with twoday Danmark a/s' information security policy
- Understand the need for twoday Danmark a/s' information security policy and guidelines and are therefore motivated to follow them
- Adhere to the guidelines and provisions for employment, including twoday Danmark a/s' information security policy and specific work methods.

It is management's responsibility to organise training, instruction, and ongoing communication about information security to achieve:

- Knowledge of twoday Danmark a/s' information security policy and the background knowledge for it
- Updated instructions on compliance with twoday Danmark a/s' information security policy to minimise the risk of security incidents
- Knowledge and motivation to enhance information security
- Specific knowledge of the security aspects of the individual employee's job, including the individual customers' solutions.

It is management's responsibility to create a culture where all information security breaches are brought to the attention of relevant parties and acted upon. It is important that all employees feel safe reporting incidents so that they can lead to learning and improvement of information security. Deliberate or repeated violations of information security may result in employment related consequences. When employment ends, twoday Danmark a/s must ensure that the employee's access to twoday Danmark a/s and possibly twoday Danmark a/s' customers' systems is terminated.

Management of assets

Inventory of assets
Procedures have been implemented to maintain an inventory of all relevant data-bearing assets. When employees leave, it is ensured that their assets are returned, cleaned of data, and updated in the inventory. All systems must have a system owner responsible for acquiring, managing the asset, and assessing risks.

Access control

Access to networks and network services
It is important for twoday Danmark a/s' employees to have access to twoday Danmark a/s' assets, even outside twoday Danmark a/s' locations. This must not increase the security risk. Therefore, rules for access to networks and network services have been established to ensure that users do not compromise security when using their equipment outside twoday Danmark a/s' network.

Access to twoday Danmark a/s' network
Access to the network requires physical presence with a connection to the network or access via VPN. Guests in the building are only allowed to connect to a dedicated guest network and not to twoday Danmark a/s' internal network. The network is also segmented so that individual companies do not have access to each other's services.

Administration of user access
As part of our information security policy, we have established rules and procedures for assigning user access, with management approval for the allocation of rights. All users must have a unique identity for personal use, and special user identities must be used for extended rights for monitoring and follow-up purposes. We use Active Directory (AD) as far as possible to control users' access to our assets. In AD, rights groups are used to ensure that users only have access to the assets they need for work-related purposes. Both internal and external users must use complex passwords according to specified requirements. The same password should not be used across different systems. Where deemed necessary based on a risk assessment, two-factor login is used. Multi-factor authentication (MFA) is always used when accessing networks and services externally. Rules are established for how employees must store passwords, including where shared access codes to assets can be stored. A password manager is used. All user profiles must be reviewed periodically (at least once a year) to identify inactive profiles or those that need to be removed or changed. When employment or temporary contracts are terminated, all associated user profiles and rights must be deactivated or withdrawn.

Cryptography

Confidential information must always be encrypted when stored on portable equipment, such as laptops and handheld computers. Access to encryption keys must be limited to the fewest possible key administrators.

Physical security and environmental security

twoday Danmark a/s' premises are not completely open; however, our customers and partners are welcome as guests. This openness must not compromise information security. Rules and procedures are established for handling guests in the building to ensure that they do not pose a threat. Guests should primarily stay on the ground floor, where there are no office workplaces. All guests must be escorted if they are not on the ground floor. Guests can be recognised by guest badges that must be worn visibly.

Video surveillance
Automatic video surveillance is established at all main entrances at twoday Danmark a/s' main premises.

Access to the server room and technical installations
Server room is outsourced to secured provider.

Access to remaining technical rooms and cross-connection points is protected with an electronic lock so that only authorised employees have access. A procedure is established for assigning access.

Clear desk policy
A clean desk policy is implemented to ensure that unauthorised persons do not have access to documents with confidential information. This includes ensuring that all workstations are automatically screen-locked with password protection when left unattended.

Security in system planning
When planning systems, security considerations must always be included. Information security requirements must be considered during the design, testing, implementation, and upgrading of IT systems, as well as during system changes.

Capacity management
The capacity of IT systems must be adjusted according to capacity requirements. twoday Danmark a/s has established procedures to ensure that capacity is continuously adjusted to meet needs.

Protection against malware

Malware controls
Procedures are implemented to ensure that active endpoint protection is installed on all computers at twoday Danmark a/s, and these are automatically updated as soon as the supplier releases new versions of both software and definitions. All connections to the outside world are protected with a firewall.

Backup
To ensure stable operation and minimise the risk of data loss, backups are made so that systems and data can be restored appropriately. Procedures are implemented to ensure secure storage and backup of data on servers. Automatic backup control is done using monitoring software. Manual backup control is performed at defined intervals for different assets.

Logging and monitoring
twoday Danmark a/s has established rules to ensure necessary logging and control. Twoday Danmark a/s follows the supplier's recommendations for the collection and protection of logs.

Communication security

twoday Danmark a/s has established rules and implemented procedures to ensure a high degree of communication security, allowing both wired and wireless networks to be used for all our systems.

Supplier relations

twoday Danmark a/s uses suppliers for various tasks. We rely on having good, reliable suppliers to provide the desired service to our customers. This includes hosting suppliers, cloud suppliers, and consultancy service providers. We use major Danish or European hosting suppliers and leading cloud suppliers' European data centres for hosting our and our customers' data. The supplier that ensures the best possible service to the customer is chosen for the specific solution. Hosting suppliers and cloud suppliers for hosting are ISO 27001 certified, and their audit statements are reviewed annually according to international standards (e.g., ISAE 3402 or SOC) and also checked against EU and UN sanction lists.

Management of information security breaches

Management has established procedures to ensure quick, effective, and methodical handling of security breaches.

Incident response process
A procedure is established to ensure that the incident management plan is continuously evaluated and adjusted based on collected experience and general industry developments. The organisation is obliged to report any observed security incident or suspicion thereof as soon as possible and through established channels. To reduce the likelihood or impact of future security incidents, past incidents are reviewed at least once a year.

Information security aspects of emergency preparedness and recovery management
System owners are responsible for preparing and maintaining appropriate emergency plans for business-critical systems to minimise downtime and costs resulting from security incidents.

Compliance

Independent review of information security
Twoday Group has started conducting external ISO audits on information security based on ISO 27001 with roll-out on a country-by-country basis.

twoday Danmark a/s does not yet conduct external ISO audits on information security, but an annual ISAE 3402 audit statement is prepared using ISO 27001 as the framework for its review of information security.

Compliance with security policies and standards
twoday Danmark a/s' information security forum has established an annual cycle where the main elements of the information security policy are reviewed at a fixed cadence. Additional reviews are conducted for significant asset acquisitions or major security incidents.

Changes during the period

twoday Danmark a/s has not had significant changes during the period from April 1, 2024, to March 31, 2025, regarding our operational services in connection with SaaS and consultancy services.

However, twoday has since the separation from Visma in 2022 been working on a coherent company strategy, whereby streamlining business operation across all countries. This has meant establishing unified Business Units across all countries as well as centralising business enablement functions like IT, HR, Finance, Marketing and Communications.

A part of the coherent company journey has let to legal merger of the former twoday entities twoday Data & AI (former Kapacity), twoday CPS (former CT Global), twoday Minds (former IT Minds) and twoday DX (former Co3) into twoday A/S – forming twoday Danmark A/S as of February 2025. The remaining entities are twoday BA-CX (former TwoMany) and twoday BA-ERP (former Relate IT).

Complementary user entity controls

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

These include:

- Customer's security requirements based on the customer's risk assessment of the task to be solved with the project or product purchased.
- Customer's own IT environment, including servers, PCs, networks, printers, licenses for third-party systems, backups, etc.
- Customer's own users, including the assignment and review of rights, necessary instructions, etc
- Testing, ensuring that the solution is tested to deliver the expected business outcome.
- Organisational effort, including implementation in the organization, establishment of organizational measures to increase the security of the solution, etc.
- Legality, including the legal basis for handling personal data, ensuring anonymized test data, etc.

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 Danmark a/s' subservice organisations.

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

Tests performed

We performed our test of controls at twoday Danmark a/s, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at twoday Danmark a/s regarding controls. Inquiries have included questions on how controls are being performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with twoday Danmark 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 Danmark a/s' control***	***Grant Thornton's test***	***Test results***
5.1.1	*Policies for information security* A set of policies for information security is defined and approved by management and then published and communicated to employees and relevant external parties.	We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant stakeholders. We have inspected that the information security policy has been reviewed and approved by the management.	No deviations noted.
5.1.2	*Review of policies for information security* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inquired into the procedure for regular review of the information security policy. We have inspected that the information security policy is reviewed, based on updated risk assessments to ensure that it still is suitable, adequate, and efficient.	No deviations noted.

A.6 Organisation of information security

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

No.	*twoday Danmark a/s' control*	*Grant Thornton's test*	*Test results*
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected an organisation chart showing the information security organisation. We have inspected that the structure is sufficient to manage the implementation and operation of information security. We have inspected the description of roles and responsibilities within the information security organisation.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.	We have inspected documentation for segregation of duties. We have inspected general organisation chart for the organisation.	No deviations noted.
6.1.5	*Information security in project management* Information security is addressed in project management, regardless of the type of project.	We have, by sample test, inspected the procedure for project management to ensure that information security is being addressed.	We have been informed that no projects have been completed within the audit period. 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 Danmark a/s' control***	***Grant Thornton's test***	***Test results***
6.2.1	*Mobile device policy* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected policy for securing of mobile devices. We have inspected, that technical controls for securing of mobile devices have been defined.	No deviations noted.
6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected the policy for securing of remote workspaces. We have inspected the underlaying security measures for protection of remote workspaces.	No deviations noted.

A.7 Human ressource security

A.7.1 Prior to employment Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities in information security.	We have inspected the procedure for onboarding new employees. We have, by sample test, inspected documentation that new employees have been informed about their roles and responsibilities in information security.	No deviations noted.

A.7.2 During employment Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inspected the information security policy for establishing requirements for employees and contractors. We have inspected, that the management, in contracts, has required that employees and contractors must observe the information security policy.	No deviations noted.
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.	We have inspected procedures for ensuring adequate education and information security training (awareness training) We have inspected that activities to develop and maintain employees' security awareness have been carried out.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected that a formal disciplinary process has been established and communicated to employees and contractors. We have, by sample test, inspected that the disciplinary process is an integrated part of the employment contract.	No deviations noted.

A.7.3 Termination and change of employment Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment or contract. We have inspected documentation that information security responsibilities and duties that remain valid after termination or change of employment have been defined and communicated. We have, by sample test, inspected that resigned employees are being informed that confidentiality agreement is still valid after termination of contract.	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets Control objective: To identify organisational assets and define appropriate protection responsibilities			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
8.1.1	*Inventory of assets* Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	We have inspected asset listings.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected list of asset ownership.	No deviations noted.

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
8.1.3	*Acceptable use of assets* Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.	We have inspected the rules for acceptable use of assets. We have inspected the procedure for working in public areas.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inspected the procedure ensuring return of assets. We have, by sample test, inspected that assets are being returned from terminated employees.	For one (1) out of the ten (10) selected samples, the return of an asset was not registered correctly. However, we have been informed that the asset was returned. No further deviations noted.

A.8.3 Media handling Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media			
No.	**twoday Danmark a/s' control**	**Grant Thornton's test**	**Test results**
8.3.1	*Management of removable media* Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	We have inspected that procedures for managing removable media are consistent with the agreed classification system.	No deviations noted.
8.3.2	*Disposal of media* Media are being disposed of securely when no longer required using formal procedures.	We have inspected procedures for disposal of media. We have, by sample test, inspected that media are being disposed of, according to the procedures.	No deviations noted.

A.9 Access control

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

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

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

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected that formalised procedures for user registration and de-registration have been established. We have, by sample test, inspected that the users' access rights have been approved. We have inspected that resigned users' access rights have been revoked.	No deviations noted.

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services.	We have inspected, that a procedure for user administration has been established. We have, by sample test, inspected that user accesses have been assigned according to the access management and control procedure. We have inquired into whether any users have changed roles or jobs during the period.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected the procedures for allocation, use and restrictions of privileged access rights. We have inspected a list of privileged users and inquired into whether access rights have been allocated based on a work-related need. We have inspected that privileged user accesses are personally identifiable. We have inspected, that periodical review of privileged access rights is being performed.	No deviations noted.
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have inspected the procedure regarding allocation of access codes to platforms. We have inspected documentation that the password policy is implemented in systems used to manage secret authentication information about users.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals.	We have inspected the procedure for regular review and assessment of access rights. We have inspected, that review and assessment of access rights is being performed twice a year.	No deviations noted.
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that resigned employees have had their access rights cancelled.	No deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
9.3.1	*Use of secret authentication information.* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected guidelines for use of secret passwords. We have inspected, that the implemented password policy is according to established guidelines.	No deviations noted.

A.9.4 System and application access control Control objective: To prevent unauthorised access to systems and applications			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
9.4.2	*Secure logon procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected the procedure for secure logon. We have inspected, that MFA (Multi Factor Authentication) has been established in connection with logon.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inquired that policies and procedures require quality passwords. We have inquired that systems for administration of access codes are configured in accordance with the requirements.	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 Danmark a/s' control	Grant Thornton's test	Test results
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy for the use of encryption. We have inspected list of updates and review of policies, and procedures where the policy for cryptography is included.	No deviations noted.
10.1.2	*Key Management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, that supports the company's use of cryptographic techniques. We have inspected that cryptographic keys are active, and that their renewal is being followed up on.	No deviations noted.

A.11 Physical and environmental security

A.11.1 Secure areas
Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

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

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

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

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	We have inspected the procedure for protection of unattended equipment.	No deviations noted.
11.2.9	*Clear desk and clear screen policy* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities has been adopted.	We have inquired into the policy of tidy desk and clear screen.	No deviations noted.

A.12 Operations security

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

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
12.1.1	*Documented operating procedures.* Operating procedures have been documented and made available to all users.	We have inspected that requirements for documentation and maintenance of operating procedures have been established. We have inspected that documentation for operating procedures is updated and accessible to relevant employees.	No deviations noted.

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure for changes in information processing facilities and systems. We have, by sample test, inspected documentation that change requests are being managed according to the established procedure.	No deviations 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.	We have inspected that relevant platforms are included in the capacity requirement procedure.	No deviations noted.

A 12.2 Protection from malware Control objective: To ensure that information and information processing facilities are protected against malware			
No.	**twoday Danmark a/s' control**	**Grant Thornton's test**	**Test results**
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inspected guidelines for controls against malware. We have inspected that controls against malware have been implemented.	No deviations noted.

A.12.3 Backup Control objective: To protect against loss of data			
No.	**twoday Danmark a/s' control**	**Grant Thornton's test**	**Test results**
12.3.1	*Information backup* Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inspected documentation, that the backup procedure has been reviewed and updated during the period. We have inspected documentation of restoretest being performed.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inquired into logging of user activities. We have inspected that logging configurations contain user activities, exceptions, faults, and incidents.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inquired about procedures for the securing of log information. We have inspected that log information is protected against tampering and unauthorised access.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged, and the logs are protected and regularly reviewed.	We have inspected procedures concerning logging of activities performed by system administrators and system operators. We have, by sample test, inspected that system administrators' and system operators' actions are being logged on servers and database systems.	No deviations noted.
12.4.4	*Clock synchronisation* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inquired into procedures for synchronisation against a reassuring time server. We have inspected, that synchronisation against a reassuring time server, has been implemented.	No deviations noted.

A.12.5 Control of operational software Control objective: To ensure the integrity of operational systems			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inspected the procedure for patching and upgrade on systems, and that is has been reviewed and updated during the period. We have inspected documentation that relevant systems are updated and patched according to specific requirements in the procedure.	No deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***twoday Danmark a/s' control***	***Grant Thornton's test***	***Test results***
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inspected the procedure regarding gathering and evaluation of technical vulnerabilities. We have, by sample test, inspected that servers, database systems and network components are patched in time.	No deviations noted.

A.13 Communications security

A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inspected that requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined. We have inspected documentation for network design.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected network charts, showing segregation of development-, test, and operations environments. We have inspected technical documentation that system environments are being segregated.	No deviations noted.

A.13.2 Information transfer
Control objective: To maintain the security of information transferred within an organisation and with any external entity

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
13.2.1	*Information transfer policies and procedures* Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.	We have inspected the procedure for managing and protection of information assets, in which transfer, and transmission of information is described. We have inspected documentation that the procedure has been reviewed and updated during the audit period.	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 Danmark a/s' control	Grant Thornton's test	Test results
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inspected that the procedure for managing suppliers and supplier agreements contains requirements of yearly monitoring and review of services rendered, are according to the contract. We have inspected, that review and assessment of relevant audit reports on significant subservice organisations have been performed.	No deviations noted.
15.2.2	*Manage changes to the third-party services* Changes in supplier services, including maintenance and improvement of existing information security policies, procedures, and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have inquired about management of changes with the supplier services, and we have inspected the documentation for handling this.	We have been informed that there have been no changes in supplier services during the audit period. No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements
Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inspected the procedure for managing security incidents. We have inspected that the procedure has been reviewed and updated during the period.	No deviations noted.

No.	twoday Danmark a/s' control	Grant Thornton's test	Test results
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inspected guidelines for reporting of information security incidents. We have, by sample test, inspected that information security incidents are being reported through appropriate management channels.	No deviations noted.
16.1.3	*Reporting security weaknesses* Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inspected guidelines for reporting of information security weaknesses. We have, by sample test, inspected that employees have reported weaknesses or suspected weaknesses in information systems and services.	No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inspected procedure for assessment of information security incidents. We have, by sample test, inspected that information security incidents have been managed according to the procedure.	No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inspected the procedure for managing information security incidents. We have inquired into whether information security breaches have occurred during the period.	We have been informed, that there have not been any information security breaches during the audit period. No deviations noted.
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about Problem Management function which analyses information security incidents in order to reduce probability of recurrence. We have inquired into whether information security breaches have occurred during the audit period.	We have been informed, that there have not been any information security breaches during the audit period, No deviations noted.

A.17 Information security aspects of business continuity management

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

No.	*twoday Danmark a/s' control*	*Grant Thornton's test*	*Test results*
17.1.1	*Planning information security continuity* Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inspected that the contingency plan has been approved by management. We have inspected that the contingency plan has been prepared, based on a risk assessment.	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 inspected that the contingency plan is maintained and updated as needed. We have inspected documentation that the contingency plan is accessible to relevant employees.	No 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 inspected documentation that risk areas in the contingency plan have been tested during the period.	No 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 Danmark a/s' control*	*Grant Thornton's test*	*Test results*
18.2.1	*Independent review of information security* Processes and procedures for information security (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have inspected documentation that independent review of the information security has been performed.	No deviations noted.
18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inspected the list of internal controls regarding compliance with policies and standards. We have, by sample test, inspected documentation that the internal controls concerning compliance with policies and procedures, have been performed.	No deviations noted.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have, by sample test, inspected documentation that review has been performed for technical compliance with policies and standards.	No deviations noted.

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

Signers

Lars Engell Berthelsen
Managing Director
d633e749-7580-4677-890b-83600de08951 *2025-07-04 09:56:00Z*

Andreas Moos
Director | IT Risk Assurance & Advisory Services
eace5ed6-cfa7-4d9e-b982-120d10f47204 *2025-07-04 09:57:14Z*

Kristian Randløv Lydolph
7b9e0bc5-648f-4c07-87a8-debb5e403de6 *2025-07-05 08:18:40Z*

Documents in the transaction

twoday - ISAE 3000-II - GDPR - 2025 - Assurance report.pdf *SHA256: 2bef9487a0fa1ed8f9c04548e21e8821d23f8e20be817a075c3d77a61066e64e*

twoday - ISAE 3402-II - 2025 - Assurance report.pdf *SHA256: 9167834147c71221e2ae3ff9781e6da645b8c2bdb52db6b00de9f79aabb8defa*