

**INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT  
FOR THE PERIOD 19 JANUARY 2024 TO 31 DECEMBER 2024  
ON THE DESCRIPTION OF DIGITAL BUSINESS SOLUTIONS  
AND THE RELATING CONTROLS AND THEIR DESIGN AND OP-  
ERATING EFFECTIVENESS**

**Abakion A/S**

Revisors kontaktoplysninger: U4378-5150ML-26NY-EPHE-1-1521-7N-1821001

## CONTENTS

<b>1. AUDITOR'S REPORT .....</b>	<b>2</b>
<b>2. ABAKION A/S STATEMENT .....</b>	<b>4</b>
<b>3. ABAKION A/S' DESCRIPTION OF DIGITAL BUSINESS SOLUTIONS .....</b>	<b>6</b>
Description of control environment .....	7
Network access control .....	9
Authentication when accessing the network.....	10
Management of Privileged Access Rights .....	10
Password Management System .....	10
Access Control to Program Source Code.....	10
Cryptography .....	10
Physical security.....	10
Management network and operations .....	10
Acquisitions, development, and maintenance of information processing systems .....	11
Outsourcing contracts .....	11
Suppliers.....	11
Incident management.....	11
Changes during the period from 18 January 2024 to 31 December 2024.....	12
<b>4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS.....</b>	<b>13</b>
Risk Assessment .....	15
A.5 Information security policies .....	16
A.6 Organisation of information security .....	17
A.7 Human Resource Security .....	19
A.8 Asset management.....	22
A.9 Access Management.....	23
A.10 Cryptography .....	26
A.11 Physical and environmental security .....	27
A.12 Operation procedures .....	28
A.13 Communications Security.....	29
A.14 System Acquisition, Development and Maintenance.....	30
A.15 Supplier relationships .....	33
A.16: Information security incident management.....	35
A.18 Compliance.....	36

## 1. AUDITOR'S REPORT

### INDEPENDENT SERVICE AUDITOR'S ASSURANCE REPORT FOR THE PERIOD THE FROM PERIOD 19 JANUARY 2024 TO 31 DECEMBER 2024 ON THE DESCRIPTION OF DIGITAL BUSINESS SOLUTIONS AND THE RELATING CONTROLS AND THEIR DESIGN AND OPERATING EFFECTIVENESS

To: The Management in Abakion A/S  
Abakion A/S customers and their auditors

#### Scope

We have been engaged to report on Abakion A/S' (the service provider) description in section 3 of Digital Business Solutions and related controls, and on the design and **operating effectiveness** of controls related to the control objectives stated in the description, throughout the period from 19 January 2024 to 31 December 2024

#### The Service Provider's Responsibilities

The service provider is responsible for preparing the description and accompanying statement in section 2, including the completeness, accuracy, and method of presentation of the description and the statement.

The service provider is responsible for providing the services covered by the description; stating the control objectives; and identifying the risks threatening achievement of the control objectives; designing and implementing effectively operating controls to achieve the stated control objectives.

#### Auditor's Independence and Quality Assurance

We have complied with the requirements of independence and other ethical requirements of the International Ethics Standards Board of Auditors' International Guidelines on the Conduct of Auditors (IESBA Code), which are based on the fundamental principles of integrity, objectivity, professional competence, and due diligence, confidentiality, and professional conduct, as well as ethical requirements applicable in Denmark.

BDO Statsautoriseret revisionsaktieselskab applies International Standard on Quality Management, 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.

#### Auditor's Responsibilities

Our responsibility is, on the basis of our actions, to express a conclusion about the service provider's description as well as about the design and operational efficiency of controls related to the control objectives set out in this description.

We have performed our work in accordance with the International Standard on Assurance Engagements 3402 on declaration duties with security checks at a service organisation. This standard requires that we plan and carry out our actions in order to obtain a high degree of certainty as to whether the description is correct in all material respects and whether the controls in all essential respects are appropriately designed and have operated effectively.

A declaration task with certainty to provide a statement about the description, design, and operational effectiveness of controls at a service provider includes performing actions to obtain evidence of the information in the service provider's description as well as of the controls' design and operational effectiveness. The actions

chosen depends on the assessment of the service provider's auditor, including the assessment of the risks that the description is not accurate and that the controls are not appropriately designed or do not operate effectively. Our actions have included tests of the operational effectiveness of such controls, which we consider necessary to provide a high degree of assurance that the control objectives set out in the description were achieved. A statement of assurance with certainty of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out therein and the appropriateness of the criteria specified and described by the service provider in section 2.

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

The service organisations' description is prepared to meet the common needs of a wide range of customers and their auditors and may not, therefore, include every aspect of Digital Business Solutions that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation 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 service providers statement in section 2. In our opinion, in all material respects:

- a. The description of Digital Business Solutions and related controls, as designed and implemented throughout the period from 19 January 2024 to 31 December 2024 is in all material aspects, accurate and
- b. The controls related to the control objectives stated in the description were suitably designed throughout the period from 19 January 2024 to 31 December 2024 and
- c. The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 19 January 2024 to 31 December 2024.

### Description of Tests of Controls

The specific controls tested, and results of those tests are listed in section 4.

### Intended Users and Purpose

This report is intended only for customers, which have used the service providers Digital Business Solutions, and their auditors who have a sufficient understanding to consider it, along with other information about controls operated by the customer themselves when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 5 February 2025

### BDO Statsautoriseret revisionsaktieselskab

Nicolai T. Visti  
Partner, State Authorised Public Accountant

Mikkel Jon Larssen  
Partner, Head of Risk Assurance, CISA, CRISC

## 2. ABAKION A/S STATEMENT

Abakion A/S provides Digital Business Solutions based on Microsoft technology to companies who seeks assistance with setting up a financial environment and provides support to the companies that Abakion has helped set up financial environments for.

The description has been prepared for Abakion A/S' customers and their auditors who have a sufficient understanding to consider Digital Business Solutions, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Abakion confirms that the accompanying description in section 3 fairly presents controls in relation to Digital Business Solutions and associated controls throughout the period 19 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

Abakion A/S confirms that the accompanying description in section 3 fairly presents controls in relation to Digital Business Solutions and associated controls throughout the period from 19 January 2024 to 31 December 2024. The criteria used in making this statement were that the accompanying description:

1. Explains the Digital Business Solutions, and how associated controls were designed and implemented, including explaining:
  - The services provided, regarding the handled groups of transactions, when it is relevant.
  - The processes in both IT and manual systems that are used to initiate the records, process and if necessary, correct the transactions and transfer these to the reports prepared for customers.
  - Relevant control objectives and controls designed to achieve those objectives.
  - Controls that what we have assumed would be implemented by the user companies with reference to the design of the system and which, if necessary to achieve the control objectives stated in the description, are identified in the description along with the specific control objectives we cannot reach ourselves.
  - Other aspects of our control environment, risk assessment process, information system (including the associated business processes) and communication, control activities and monitoring controls that have been relevant to the processing and reporting of customer transactions.
2. Includes relevant details of changes to the controls relating to the service providers Digital Business Solutions during the period from 19 January 2024 to 31 December 2024.
3. Does not omit or distort information relevant to the scope of the controls described relating to Digital Business Solutions considering that the description is prepared to meet the general needs of a wide range of customers and their auditors and therefore cannot include every aspect of Digital Business Solutions that the individual customer may consider of importance to their special environment.

Abakion A/S confirms that controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 19 January 2024 to 31 December 2024. The criteria we used in making this statement were that:

1. The risks that threatened achievement of the control objectives stated in the description were identified.
2. The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved.
3. 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 19 January 2024 to 31 December 2024.

Copenhagen, 5 February 2025

**Abakion A/S**

Kenneth Kryger Gram  
CEO

### 3. ABAKION A/S' DESCRIPTION OF DIGITAL BUSINESS SOLUTIONS

#### Abakion A/S

Abakion A/S is a Danish-owned company that develops software products based on Microsoft's business platforms (ERP, CRM, BI solutions and e-Commerce) and assists customers with support on a number of online systems for both municipalities and various industries in the private market. Abakion A/S has offices in Copenhagen and Aarhus.

Abakion's ca. 200 employees specialized in software development, support, and consulting, and are organized into a product department, consulting business, finance department and an administration department.

Abakion's consulting business includes the Frontdesk & Cloud subdivision, which is overall responsible for the operation of Abakion's IT systems, IT security and technical and organizational security measures.

For Abakion, it is therefore important to ensure:

- Confidentiality - a confidential treatment, including transmission and storage of information, where only authorized internal and external users have access, and where the users' access is limited to what is necessary in relation to a work-related need.
- Integrity - a reliable and correct functionality in our IT systems, which minimizes the risk of incorrect information due to internal or external conditions.
- Accessibility - the availability and capacity of IT systems must reflect our need for well-functioning IT systems and access to information.

Abakion has therefore adopted this IT and information security policy (hereinafter "IT security policy or ISP"). The IT security policy forms the overall management-approved basis for the IT security work in Abakion.

IT security is defined in the following as being all security measures aimed at protecting electronic data, personal data, information, and IT-related assets used by Abakion.

Management of the personal data security as well as the technical and organizational safety precautions and controls are structured in the following segments, for which there are defined controls.

ISO 27001	Control activities
Risk assessment	<ul style="list-style-type: none"> <li>• Risk assessment</li> </ul>
A.5: Information security policies	<ul style="list-style-type: none"> <li>• Information Security Policy</li> <li>• Review of information security policy</li> </ul>
A.6: Organisation of information security	<ul style="list-style-type: none"> <li>• Roles and responsibilities</li> <li>• Segregation of duties</li> <li>• Mobil device policy</li> <li>• Remote workplaces and remote access to systems and data</li> </ul>
A.7: Human resource security	<ul style="list-style-type: none"> <li>• Recruitment of employees</li> <li>• Training and instruction of employees who process personal data</li> <li>• Non-disclosure and confidentiality agreements</li> <li>• Resignation of employees</li> </ul>
A.8: Asset management	<ul style="list-style-type: none"> <li>• Inventory of assets</li> </ul>
A.9: Access management	<ul style="list-style-type: none"> <li>• User registration and deregistration</li> <li>• Allocation of user access</li> <li>• Management of privileged access rights</li> <li>• Review of user access rights</li> <li>• Use of Secret Authentication Information</li> <li>• Procedure for secure log-on</li> <li>• Logical access control</li> </ul>
A.10: Cryptography	<ul style="list-style-type: none"> <li>• Policy for encryption</li> <li>• Administration of keys</li> </ul>

ISO 27001	Control activities
A.11: Physical and environmental security	<ul style="list-style-type: none"> <li>• Policy for clean desk and desktop</li> </ul>
A.12: Operations security	<ul style="list-style-type: none"> <li>• Maintaining system software</li> <li>• Antivirus program</li> <li>• Data backup</li> <li>• Logging in systems, databases, and networks, including logging of the use of personal data</li> <li>• Surveillance</li> </ul>
A.13: Communication security	<ul style="list-style-type: none"> <li>• Network security</li> <li>• firewall</li> <li>• External communication connections</li> </ul>
A.14: Acquisition, development, and maintenance of systems	<ul style="list-style-type: none"> <li>• Development and maintenance of systems</li> <li>• Information security in development and changes</li> <li>• Separation of development-, test and production environment</li> <li>• Support assignments</li> </ul>
A.15: Supplier relationships	<ul style="list-style-type: none"> <li>• Sub service providers agreements and instructions</li> <li>• Control with service organisations</li> </ul>
A.16: Information security incident management	<ul style="list-style-type: none"> <li>• Responsibilities and procedures</li> <li>• Registration of breaches of information security</li> </ul>
A.18: Compliance	<ul style="list-style-type: none"> <li>• Identification of applicable legislation and contractual requirements</li> </ul>

## DESCRIPTION OF CONTROL ENVIRONMENT

### Description of Abakion A/S IT systems

Abakion has chosen Microsoft as subcontractor in relation to storage and settlement of services, systems, and data. Microsoft has put in place procedures to ensure that databases are encrypted and that the same applies to backups. Abakion monitors Microsoft through reviewing SOC2 reports annually. Microsoft handles customer solutions in Microsoft Online and ensures that they undergo security checks and penetration tests performed by Microsoft, which ensures that systems are put in place to identify and address technical vulnerabilities in applications, services, and infrastructure, so that loss of confidentiality, integrity and availability of systems and data is avoided.

### Management of IT

Abakion A/S has an overall strategy for the use and purchase of IT equipment. We use a single large supplier that ensures a "single point of contact", and thus our history is gathered in one place. This helps to give us a quick overview of acquisitions and better sparring around new acquisitions, as the supplier can guide us based on previous acquisitions.

In connection with the performance of our service, it may be necessary to make use of external assistance. We always ensure that agreements with external service providers and out-source providers are formalized where relevant and that partners are familiar with our IT security policy.

Should an emergency arise, Microsoft has prepared a contingency plan, which is described in another document. The IT security work in Abakion is divided into the following core areas:

- The IT security policy describes the overall framework for the IT security policy in Abakion.
- IT business procedures and procedures are the specific guidelines and instructions that must be followed by the employees in the daily work, for example approval flow.

Operating and outsourcing guidelines describe the detailed guidelines, rules, instructions, and controls, for example minimum safety requirements for setting up system parameters. This will apply in relation to internal operations as well as operations handled by external parties.



### Risk assessment and management

To focus the efforts of the IT security work at Abakion, we work according to a structured approach to risk management. The result of the risk management, including assessment of risks, is made in Abakion's management.

The management is also immediately informed of significant deviations in the current threat picture and the adaptation that this leads to in relation to the focus areas and controls. Minor deviations are collected and reported periodically to Abakion's Executive Board and are also included in the annual reporting.

To protect Abakion against the negative consequences of IT threats, the IT security work must be based on a risk assessment of the threats that Abakion has identified by:

- Abakion continuously assesses potential IT threats, which are analyzed periodically. Abakion must continuously decide how these risks and threats are countered.
- Suppliers have a significant role in participating in the preparation of risk assessments in relation to the development projects and operational tasks for which they are responsible. Suppliers are thus responsible for collecting and responding to changing risks and new security incidents and communicating this to Abakion.
- Abakion must make demands on partners and suppliers that IT contingency plans have been prepared and documented, and that these have been tested in collaboration with Abakion. Tests must be approved by Abakion's management.

### Security Policy

Abakion's IT security work is rooted in "good IT practice" within information security and is based on the ISO 27001 standard and the associated ISO 27002 control framework. This, among other things, to live up to the requirements of an ISAE3000 and a ISAE3402 audit statement.

Several overall requirements for IT security have been established to ensure that there is a basis for being able to maintain a level of security that is expected to ensure critical infrastructure and applications for Abakion. The level of security is ensured by:

- There is a managerial anchoring of IT security.
- It has been determined how Abakion meets relevant regulatory and regulatory requirements.
- The organization has a unique responsibility for all areas covered by the IT security policy, knowing that it can be difficult to maintain an organizational separation of functions with the number of employees that Abakion has at its disposal. If function separation is not possible, compensatory controls have been prepared.
- Ongoing information campaigns are carried out on the Abakion intranet and at house meetings to ensure focus on each employee's responsibility.
- All employees are instructed in the parts of the IT security policy, IT business procedures, procedures, etc. that are relevant to their area of work.
- Interfaces and division of responsibilities with suppliers are precise and established.
- External parties have become aware of and undertake to comply with the current IT security policies, business procedures, rules, and guidelines in the cooperation with Abakion.
- Continuous checks are carried out to ensure that significant IT subcontractors comply with the requirements set by Abakion, just as an assessment is made on an ongoing basis of the suppliers' competencies to be able to handle the specific task.
- Contracts with suppliers that do not meet the requirements of the IT security policy are updated based on a risk-based consideration.
-

### Employee safety / HRM

HR receives and conducts the screening of applications before employment and is obliged to ensure the deletion of the information about the candidates in every 6 months. HR needs to send the e-mail notification to every employee and remind them to delete the data related to the candidates. Upon recruitment HR needs to present the contract which includes the paragraphs about the personal data protection to new employees. After resignation of an employee, the contract should be still considered valid and off-boarded employees need to be informed correspondingly.

### HR - duty of confidentiality

Upon recruitment new employees need to sign the contract which includes paragraphs about the duty of confidentiality. By signing the contract, new employees demonstrate their commitment to the duty of confidentiality. In certain cases, upon request of a customer the separate confidentiality agreement will be signed.

### Management of information-related assets

Abakion must appear as a reliable organization that ensures that IT services are available, and that information is protected. This is ensured by:

- New purchases of importance for information security are based on business-related needs and subject to an initial risk and impact assessment.
- Development and modification of IT systems takes place after a formalized process in which Abakion's needs and requirements are described. The process must ensure operational stability, traceability, and testability of the system. In addition, the process must ensure the preparation of system, operating and user documentation.
- Personal information, business-critical information and confidential information are processed in accordance with the law and commercially as well as ethically correct. The information is assessed in a life cycle from registration, processing, and storage to disposal.
- There is a system owner who ensures that systems are specified, tested, and implemented, and that controls are implemented that correspond to the risk picture.
- The IT environment is secured against undesirable events such as physical damage, operational disruptions, losses, unauthorized changes, and use.
- Unauthorized access to the IT environment is not achieved and reassuring functional separation is maintained.
- Confidentiality and personal data protection are included in all development initiatives as a natural part of the work process throughout the life cycle.
- Appropriate malicious code testing and unauthorized attacks on Abakion's applications and infrastructure are identified in relation to identified risks.

### Access Control

Abakion maintains a user account access control management process to control user access to IT-systems. User accounts are unique and personalized so that any action can be traced and linked to individual users. IT must ensure compliance with business requirements for traceability, e.g., by securing logs that can be correlated to control users' action in applications and on the network.

User rights are defined in a way that access rights are granted only when necessary for the fulfilment of the user's duties. Access to confidential and personal data must only be allowed for work needed purposes. Processes must be put in place that ensure an adequate user administration, including periodic reviews and termination of accounts on leave or change in employment.

### Network access control

The default setting of network access control systems and firewalls must be configured to "deny all", i.e., allow only access to resources that are explicitly permitted.

**Authentication when accessing the network**

A two-factor authentication mechanism must be in place to protect all access to internal network and application resources from non-Abakion networks.

**Management of Privileged Access Rights**

The system administrative and normal accounts must be separated. The allocation and use of privileged access rights, i.e., system administration permissions, is strictly controlled. IT administrative rights must be authorized by the management on proposition from the Head of IT. All IT-administrators must have a unique identity for tasks that require high privileges. Given their higher risk nature, the users with privileged access must be reviewed by internal IT at more frequent intervals than regular user rights.

**Password Management System**

Abakion has implemented requirements for user account password management to ensure that passwords meet the required secure level.

**Access Control to Program Source Code**

Access to program source code must be restricted. Source code and source code libraries (including designs, specifications, verification plans and validation plans) must be protected by access control system. The same applies to source code for applications being developed.

Controls must include consideration for:

- Maintenance and copying of source code must follow a documented change control procedure.
- Source code printouts must be securely stored.
- Source code must not be stored in the production environment.

Control environment will be established with documented, regular controls.

**Cryptography**

Information, data, and documents in portable computers must be hard drive encrypted in accordance with industry standards. Emails containing confidential information including personal data must be encrypted under transmission in flight. (Minimum TLS v. 1.2)

Any connection between Abakion IT systems and customer IT systems, must be protected by https. (Minimum TLS version 1.2).

**Physical security**

To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities, Abakion has implemented physical entry controls. Physical entry controls aim to protect physical locations and restricted secure areas.

Secure areas are protected by the appropriate entry controls, e.g., alarms, locks, and access control cards to ensure that only authorized personnel are allowed access. Visitor access is handled by ensuring enrolment and pick-up at the reception.

**Management network and operations**

Abakion has a guest network that runs around the primary network. Networks can be managed via management dashboard. The IT department has access to this. All hosts on the network must be documented and visible on the management dashboard. All computers' hard drives must be encrypted with Bitlocker. This means that data is not available should a computer be stolen. Microsoft Defender Antivirus, which is in place on all computers, includes Firewall & Network protection.

Abakion ensures that the IT delivery takes place in accordance with recognized "good IT practice" for the relevant areas, including daily administration, system planning, monitoring, change management, general and incident reporting, etc. Abakion is responsible for following up that the IT service meets the requirements and expectations that Abakion has set. Abakion has no servers on the premises, all customer data is in the cloud. Abakion's physical network is divided into several different VLANs. Abakion has an IT room where the network is managed. This room needs to remain available only to the IT department and specially selected employees.

Abakion needs to monitor its own and customers' cloud servers daily. Every morning, Pulseway is reviewed for alarms that were triggered after the employees left office, the day before. Pulseway provides visible notifications, urgent events will be handled without unnecessary delay. All employees can create a request via e-mail or go directly to the IT department if they require help updating software. The IT department needs to roll out software updates to employees if there are important changes to the individual software. Abakion uses a program to monitor and manage all employees' computers. In that way the company can monitor which version of Windows users are running. In the case of outdated software, an email will be sent to the person who is asked to update their software immediately.

### **Acquisitions, development, and maintenance of information processing systems**

All suppliers who handle a responsibility and/or tasks, are subject to the purpose and scope of the IT security policy. Abakion may decide to outsource activities, including using cloud solutions. Outsourcing of significant areas of activity can only take place by an executive board decision, considering all relevant regulatory requirements and regulations in general.

### **Outsourcing contracts**

The contract must contain an IT security instruction that describes the desired IT security level for Abakion's systems and data, as well as a requirement that the supplier complies with Abakion's IT security policy and always set of rules. Abakion must ensure ongoing control and follow-up on compliance with this. Requirements for outsourcing contracts also apply to external consultants, IT deliveries and other partners.

### **Suppliers**

It is ensured that statutory inspections of service providers are carried out on an ongoing basis, based on the risk assessment carried out in accordance with the individual service provider.

Abakion must ensure that agreements and instructions described in service provider agreements are carried out correctly and within the framework of the law. Furthermore, it must be ensured that the fixed annual supervision obligation is fulfilled by physical supervision, audit statements or anything else agreed in the service provider agreement is fulfilled. This applies to Abakion as data controller and to Abakion as service provider, and in relation to sub-service providers. When Abakion use sub service providers that includes a data processing agreement, Abakion has the obligation at least once pr. Year, to control sub service providers internal audit like SOC1, ISAE3000, ISAE3402 or other audit report, to make sure that the sub processor meets the requirement regarding. organizational and technical measures as described in the data processing agreement.

### **Incident management**

In the event of any security breach, incident or attempt at the same, the management is contacted and the responsible assesses and documents the next step. It must be ensured that all incidents that can be reported, unintentional as accidental and intentional that may be considered to have an impact on general IT security must be registered in the incident system and handled according to applicable processes. Thereafter, Abakion shall assist with assistance of any relevant and agreed nature, by identifying and remedying service providers, and subsequently ensuring an alert program aimed at employees, for security against recurrence.

**CHANGES DURING THE PERIOD FROM 19 JANUARY 2024 TO 31 DECEMBER 2024**

Abakion has not made significant changes of the Digital Business Solutions and the relating technical and organizational security measures and other controls during the period from 19 January 2024 to 31 December 2024.

## 4. CONTROL OBJECTIVES, CONTROLS, TEST AND RESULTS OF TESTS

### Objective and scope

BDO has carried out the work in accordance with ISAE 3402 on assurance engagements relating to controls at a service organisation.

BDO has performed procedures to obtain evidence of the information in Abakion A/S description of Digital Business Solutions and the design and the operating effectiveness of these controls. The procedures performed depend on BDO's assessment, including the assessment of the risks that the description is not fairly presented and that the controls are not suitably designed or operating effectively.

BDO's test of the design and operating effectiveness of controls has included the control objectives and related control activities selected by Abakion A/S, and which are described in the following.

In the check form, BDO has described the tests performed which were considered necessary to obtain a reasonable degree of assurance that the stated control objectives were achieved and that the related controls were suitably designed and operated effectively throughout the period from 19 January 2024 to 31 December 2024.

### Test procedures

Tests of the design of technical and organisational security measures and other controls, the implementation and effectiveness hereof were performed by inquiry, inspection, observation, and re-performance.

Type	Description
Inquiry	<p>Inquiries of relevant personnel at Abakion A/S have been performed for all significant control activities.</p> <p>The purpose of the inquiries was to obtain knowledge and further information about implemented policies and procedures, including how the control activities are performed, and to obtain confirmed evidence of policies, procedures, and controls.</p>
Inspection	<p>Documents and reports, which include information about the performance of the control, have been read for the purpose of assessing the design and monitoring of the specific controls, i.e., whether the design of the controls is such that they are expected to be effective if implemented, and whether the controls are sufficiently monitored and checked at suitable intervals.</p> <p>Tests have been performed of significant system structures of technical platforms, databases, and network equipment to ensure that controls have been implemented, including for example assessment of logging, back-up, patch management, authorisations and access controls, data transmission, and inspection of equipment and locations.</p>
Observation	<p>The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.</p>
Re-performance	<p>Controls have been re-performed to obtain additional evidence that the controls operate as assumed.</p>

With respect to the services provided by Microsoft within Microsoft Azure, we have from independent auditor received the SOC 1 report for the sub data providers' technical and organizational security measures and other controls for the period from 1 July 2023 to 30 Juni 2024.

With respect to the services provided by Continia Software within operation of Document Capture and Expense Management, we have from independent auditor received the ISAE 3402 assurance report for the sub data provider's technical and organizational security measures and other controls for the period from 1 May 2023 to 30 April 2024.

With respect to the services provided by Global Mediator within software engineering, we have from independent auditor received the ISO 27001 certificate for the sub data provider's technical and organizational security measures and other controls for the period from 3 July 2023 to 8 July 2026.

With respect to the services provided by Atlassian within project and task management, we have from independent auditor received the SOC 2 report for the sub data providers' technical and organizational security measures and other controls for the period from 1 October 2023 to 30 September 2024.

With respect to the services provided by Zendesk within registration and handling of support, we have from independent auditor received the ISO 27001 certificate for the sub data provider's technical and organizational security measures and other controls for the period from 26 April 2024 to 14 April 2027.

These sub-service provider's relevant control objectives and related controls are not included in Abakion A/S' description of services and relevant controls related to operation of Abakion A/S' Digital Business Solutions. Accordingly, we have solely assessed the report and tested the controls at Abakion A/S that monitor the operating effectiveness of the sub-service provider's controls.

### **Result of test**

The result of the test made of technical and organisational measures and other controls has resulted in the conclusions specified on the following pages.

An exception exists when:

- Technical and organisational measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational measures and other controls related to a control objective are not suitably designed and implemented or did not operate effectively throughout the period.

Risk Assessment		
<b>Control objectives</b> ▶ To ensure that an annual risk assessment, which forms basis for business motivated implementations of controls, is performed.		
Control Activity	Test performed by BDO	Result of test
<b>Risk assessment</b> <ul style="list-style-type: none"> <li>▶ A risk assessment of Abakion's solutions is carried out based on potential risks to the availability, confidentiality, and integrity of systems and data.</li> <li>▶ The vulnerability of systems and processes is assessed based on identified threats.</li> <li>▶ Risks are minimised based on the assessment of their probability, consequence, and derived implementation costs.</li> <li>▶ Risk assessments are updated regularly as needed, but at least once a year.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We inspected Abakion's risk assessment and associated procedure and observed that it has been during the declaration period, and it is based on data availability, probability and derived implementation costs based on the potential risks.</p> <p>We have inspected the risk assessment and observed that it covers identified vulnerabilities of systems and processes.</p> <p>We have inspected the risk procedure and risk assessment and observed that risks are minimised based on the assessment of probabilities, consequences, and derived implementation costs.</p>	<p>No exceptions noted.</p>



A.5 Information security policies		
<b>Control objectives</b> ▶ <i>To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations.</i>		
Control Activity	Test performed by BDO	Result of test
<b>Policies for information security</b> <ul style="list-style-type: none"> <li>▶ The service provider has developed and implemented an information security policy.</li> <li>▶ The service provider has developed and implemented a policy, containing a guarantee of assistance and obligation to achieve compliance with relevant requirements, laws, and regulations.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We inspected Abakion's information security policy and observed that it has been updated in during the declaration period.</p> <p>We have observed that the information security policy, include guarantee of assistance and obligation to achieve compliance with relevant requirements, laws and regulations has been made and implemented.</p>	No exceptions noted.
<b>Review of information security policy</b> <ul style="list-style-type: none"> <li>▶ The service provider's information security policy is reviewed and updated at least once a year.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We inspected Abakion's information security policy and observed that it has been updated during the declaration period.</p>	No exceptions noted.

A.6 Organisation of information security		
<b>Control objectives</b> ▶ To establish a managerial basis for being able to initiate and control the implementation and operation of information security in the organisation. ▶ To ensure remote workstations and use of mobile equipment.		
Control Activity	Test performed by BDO	Result of test
<b>Roles and responsibilities</b>  ▶ The service provider has documented and established management of information security. ▶ All responsibility areas for information security have been defined and distributed.	We have made inquiries of relevant personnel at the service provider.  We have observed that the information security policy, has been implemented and approved by the management.  We have inspected the information security policy and observed that responsibility for information security has been assigned and distributed.	No exceptions noted.
<b>Segregation of duties</b>  ▶ The conflicting functions and responsibilities of the service provider are separated, to the extent possible, considering the size of the company, to reduce the possibility of unauthorized or unintentional use, alteration or misuse of data.	We have made inquiries of relevant personnel at the service provider.  We have inspected the technical set-up for the different roles at Abakion and observed there is a segregation of duties between the responsibilities of Abakion's employees.	No exceptions noted.
<b>Mobile device policy</b>  ▶ The service provider has developed and implemented a policy and supportive security measures to manage the risks of personal data arising from the use of mobile devices.	We have made inquiries of relevant personnel at the service provider.  We have inspected Abakion's mobile device policy and observed that security measures are in place.	No exceptions noted.

A.6 Organisation of information security		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To establish a managerial basis for being able to initiate and control the implementation and operation of information security in the organisation.</li> <li>▶ To ensure remote workstations and use of mobile equipment.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Remote workplaces and remote access to systems and data</b> <ul style="list-style-type: none"> <li>▶ All mobile devices used to process personal data in a work context must have antivirus installed and updated.</li> <li>▶ Remote access to the service provider's systems and data is encrypted.</li> <li>▶ Remote access must go via two-factor authentication.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>By random sampling, we have inspected that antivirus is installed and updated.</p> <p>We have inspected Abakion's policy for organising information security and observed that remote access to Abakion's systems and data takes place via a remote gateway.</p> <p>We have inspected the procedure for remote access to customers' servers and observed that RDP is used to access Abakion's systems, and that RDP alongside VPN or Gateway is used to access customers' data.</p> <p>We have inspected that remote access goes via two-factor authentication.</p>	<p>No exceptions noted.</p>

A.7 Human Resource Security		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To ensure that employees and contracting parties understand their areas of responsibility and are suitable for the roles for which they are assigned.</li> <li>▶ To ensure that employees and contracting parties are aware of and meet their information security responsibilities.</li> <li>▶ To protect the organisation's interests as part of changes to or termination of the employment.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Recruitment of employees</b> <ul style="list-style-type: none"> <li>▶ The service provider performs screening of potential employees before employment in the form of interviews and test cases.</li> <li>▶ The service provider performs a background check of all job candidates in accordance with business requirements and the function to be held by the employee.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for HR and observed that candidates must be screened.</p> <p>By random sampling we have inspected that Abakion performs screening of potential candidates before employment</p> <p>We have inspected Abakion's employment contract template.</p> <p>By random sampling, we have inspected that the employment contract template is used when an employee is hired.</p>	No exceptions noted.
<b>Training and instruction of employees in information security</b> <ul style="list-style-type: none"> <li>▶ The service provider conducts instruction training of new employees in accordance with information security.</li> <li>▶ The service provider carries out ongoing training of employees in accordance with information security and data protection as well as handling thereof.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for HR and observed that employees must receive training in data protection and information security.</p> <p>By random sampling we have inspected that new employees receive data protection and information security training as part of their onboarding.</p> <p>We have inspected that Abakion annually carries out training for all employees in data protection and information security.</p>	No exceptions noted.

A.7 Human Resource Security		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To ensure that employees and contracting parties understand their areas of responsibility and are suitable for the roles for which they are assigned.</li> <li>▶ To ensure that employees and contracting parties are aware of and meet their information security responsibilities.</li> <li>▶ To protect the organisation's interests as part of changes to or termination of the employment.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Non-disclosure and confidentiality agreements</b> <ul style="list-style-type: none"> <li>▶ All employees working with confidential data – including personal data – have signed a confidentiality agreement.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for HR and observed that employees must sign an employment contract that contains a confidentiality agreement.</p> <p>We have inspected Abakion's employment contract template and observed that it contains a confidentiality agreement.</p> <p>By random sampling, we have inspected that employees have signed an employment contract that contains a confidentiality agreement.</p>	No exceptions noted.
<b>Resignation of employees</b> <ul style="list-style-type: none"> <li>▶ The service provider has prepared and implemented a procedure for offboarding employees.</li> <li>▶ Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's Procedure for HR and observed that it contains a procedure for resignation.</p> <p>We have inspected Abakion's resignation template.</p> <p>By random sampling, we have inspected that resigning employees have returned assets and user access terminated.</p> <p>We have inspected Abakion's Procedure for HR and observed that resigning employees are informed that the signed confidentiality agreement is still valid.</p>	No exceptions noted.

## A.7 Human Resource Security

### Control objectives

- ▶ *To ensure that employees and contracting parties understand their areas of responsibility and are suitable for the roles for which they are assigned.*
- ▶ *To ensure that employees and contracting parties are aware of and meet their information security responsibilities.*
- ▶ *To protect the organisation's interests as part of changes to or termination of the employment.*

Control Activity	Test performed by BDO	Result of test
	By random sampling, we have inspected that employees are informed that the signed confidentiality agreement is still valid upon resignation.	

A.8 Asset management		
<b>Control Objective</b> ▶ To identify the organisation's assets and define appropriate responsibilities for its protection.		
Control Activity	Test performed by BDO	Result of test
<b>Inventory of assets</b> ▶ Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	We have made inquiries of relevant personnel at the service provider.  We have inspected Abakion's inventory of assets list in relation to information and information processing facilities.	No exceptions noted.

A.9 Access Management		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To restrict access to information and information processing facilities.</li> <li>▶ To ensure access for authorised users and prevent unauthorised access to systems and services.</li> <li>▶ To make users responsible for safeguarding their authentication information.</li> <li>▶ To prevent unauthorised access to systems and applications.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>User registration and deregistration</b> <ul style="list-style-type: none"> <li>▶ The service provider has implemented an administration procedure that ensures that user creations and closures follow a controlled process and that all user creations are authorised.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for access management and observed that creations and closures follow the procedure.</p> <p>By random sampling, we have inspected that an employee is granted access based on a work-related need.</p> <p>By random sampling, we have randomly inspected that an employee's access is terminated upon resignation.</p>	No exceptions noted.
<b>Allocation of user access</b> <ul style="list-style-type: none"> <li>▶ The service provider has a record of users with access to systems with personal information.</li> <li>▶ User rights are allocated based on a work-related-need.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have observed that while a list of users with access to customers systems is not kept, one can from Abakion's system identify who has access to customers' systems and thereby access to systems with personal information.</p> <p>By random sampling, we have inspected that an employee is granted access based on a work-related need</p>	No exceptions noted.
<b>Management of privileged access rights</b> <ul style="list-style-type: none"> <li>▶ Privileged accounts (administrative rights) to systems are granted based on a work-related need.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for access management.</p>	No exceptions noted.



A.9 Access Management		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To restrict access to information and information processing facilities.</li> <li>▶ To ensure access for authorised users and prevent unauthorised access to systems and services.</li> <li>▶ To make users responsible for safeguarding their authentication information.</li> <li>▶ To prevent unauthorised access to systems and applications.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
	We have inspected that Abakion grants administrative rights to systems based on work-related need.	
<b>Review of user access rights</b> <ul style="list-style-type: none"> <li>▶ Users and user rights are reviewed annually.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that Abakion reviews users and user rights annually, and we have observed that the review has been conducted during the declaration period.</p>	No exceptions noted.
<b>Use of secret authentication information</b> <ul style="list-style-type: none"> <li>▶ The service provider has established rules for password requirements, which must be followed by all employees as well as external consultants.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakions password policy and observed that the password requirements are enforced on all employees and external consultants.</p>	No exceptions noted.
<b>Procedure for secure log-on</b> <ul style="list-style-type: none"> <li>▶ The service provider has established logical access control for systems with personal data, including two-factor authentication.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that Abakion has established logical access control for systems with two-factor authentication.</p>	No exceptions noted.

## A.9 Access Management

### Control objectives

- ▶ *To restrict access to information and information processing facilities.*
- ▶ *To ensure access for authorised users and prevent unauthorised access to systems and services.*
- ▶ *To make users responsible for safeguarding their authentication information.*
- ▶ *To prevent unauthorised access to systems and applications.*

Control Activity	Test performed by BDO	Result of test
<b>Logical access control</b> <ul style="list-style-type: none"> <li>▶ A log is kept for all accesses to systems and data.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that all access to systems and data is logged.</p>	No exceptions noted.

A.10 Cryptography		
<b>Control objectives</b> ▶ To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information and personal data.		
Control Activity	Test performed by BDO	Result of test
<b>Policy for the use of cryptography</b> <ul style="list-style-type: none"> <li>▶ The service provider has implemented an encryption policy for encrypting personal data. The policy defines the strength and protocol of encryption.</li> <li>▶ Portable media is encrypted.</li> <li>▶ Encryption is used for the transmission of confidential and sensitive personal information via the internet and e-mail.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's encryption policy and observed that personal data must be encrypted.</p> <p>We have inspected Abakion's encryption policy and observed that portable media with personal data must be encrypted.</p> <p>By random sampling, we have inspected that portable media are encrypted.</p> <p>We have inspected Abakion's encryption policy and observed that e-mails must be encrypted if confidential or sensitive personal data is transmitted.</p>	No exceptions noted.
<b>Administration of keys</b> <ul style="list-style-type: none"> <li>▶ The encryption keys are stored in a location other than where encrypted data is stored.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's policy for encryption and observed that keys must be stored in another location.</p> <p>We have inspected that encryption keys are stored in a location that is different from where encrypted data is stored.</p>	No exceptions noted.

A.11 Physical and environmental security		
<b>Control objectives</b> ▶ To ensure the correct and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information and personal data.		
Control Activity	Test performed by BDO	Result of test
<b>Policy for clean desk and desktop</b>  ▶ The Screen lock is activated after 15 minutes. ▶ Employees activate screen lock when they leave their computer.	We have made inquiries of relevant personnel at the service provider.  We have inspected Abakion's domain policy and observed that the screen lock is automatically activated after 15 minutes.  We have inspected Abakion's employee handbook and observed that the clients must be locked when leaving the office.	No exceptions noted.

A.12 Operation procedures		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To ensure correct and secure operation of information processing facilities.</li> <li>▶ To ensure that information and information processing facilities are protected against malware.</li> <li>▶ To protect against loss of data.</li> <li>▶ To register incidents and provide evidence.</li> <li>▶ To ensure the integrity of operating systems.</li> <li>▶ To prevent the exploitation of technical vulnerabilities.</li> <li>▶ To minimise the effect of audit activities on operation systems.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Maintaining system software</b> <ul style="list-style-type: none"> <li>▶ The service provider has implemented a process for updating system software with regards to ensuring the systems' availability and security.</li> <li>▶ Operating systems software on workstations are regularly updated.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for maintaining system software and observed that system software on mobile devices, servers, SaaS platforms and on-premises is continuously updated.</p> <p>By random sampling, we have inspected that Abakion continuously updates system software on workstations.</p>	No exceptions noted.
<b>Antivirus program</b> <ul style="list-style-type: none"> <li>▶ Antivirus software is installed on all workstations.</li> <li>▶ Antivirus software is constantly updated and updated with the latest version.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that antivirus is installed on alle workstations.</p> <p>By random sampling, we have inspected that antivirus is installed and continuously updated on the computer.</p>	No exceptions noted.
<b>Logging in to systems, databases, and networks, including logging of the use of personal data</b> <ul style="list-style-type: none"> <li>▶ All successful and unsuccessful attempts to access the service provider's systems and data are logged.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that all successful and unsuccessful attempts to access Abakion's systems and data are logged.</p>	No exceptions noted.

A.13 Communications Security		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ To ensure protection of information in networks and of supporting information processing facilities.</li> <li>▶ To maintain information security at internal transmission in an organisation and to an external entity.</li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Network security</b> <ul style="list-style-type: none"> <li>▶ Network topology is structured according to best practise so that servers that manage the application cannot be reached directly from the internet.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakions physical network and observed that Abakions network is separated so internal servers cannot communicate directly with the internet.</p> <p>We have observed that firewalls have been set-up on Abakion's VLAN.</p>	No exceptions noted.
<b>Firewall</b> <ul style="list-style-type: none"> <li>▶ The service provider only uses services/ports which are needed.</li> <li>▶ Firewalls are configured and validated periodically as needed to ensure that services/ports only are opened as they are needed.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected relevant documentation and observed that Abakion only uses services/ports which are needed.</p> <p>We have inspected that firewalls are configured and observed that firewalls are validated periodically and as needed.</p>	No exceptions noted.
<b>External communication connections</b> <ul style="list-style-type: none"> <li>▶ External connection to systems and databases, which are used to process personal data, occurs through secure firewall and VPN.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's policy for organising information security and observed that remote access to the Abakion's systems and data takes place via a remote gateway.</p>	No exceptions noted.

A.14 System Acquisition, Development and Maintenance		
Control objectives		
<p>▶ To ensure that information security is prepared and implemented within information systems' development life cycle.</p>		
Control Activity	Test performed by BDO	Result of test
<p><b>Development and maintenance of systems</b></p> <ul style="list-style-type: none"> <li>▶ The service provider works based on the relevant principals in development and maintenance assignments.</li> <li>▶ Risk evaluations of systems changes are done, to ensure data protection by design.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that Abakion works based on security-by-design principles in development and maintenance assignments.</p> <p>We have inspected Abakion's procedure for risk assessments and observed that major changes must be risk evaluated to ensure data protection by design.</p> <p>Upon enquiry, we have been informed that no major changes have been conducted during the declaration period. Thus, we have not been able to test the implementation and effectiveness.</p>	<p>We have noted that a procedure for risk assessments has been implemented. However, we have not been able to comment on the implementation and effectiveness of the control, as no major changes have been conducted during the declaration period.</p> <p>No exceptions noted.</p>
<p><b>Information security in development and changes</b></p> <ul style="list-style-type: none"> <li>▶ The service provider works based on the principles of security-by-design in development and maintenance assignments.</li> <li>▶ Rollback is ensured through version-controlled source codes in case of failures in the production environment.</li> <li>▶ Users are generally created with lowest level of user rights.</li> <li>▶ Solely the service provider's developers and project leaders with a work-related need have access to the source codes.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that Abakion works based on security-by-design principles in development and maintenance assignments.</p> <p>We have inspected Abakion's procedure for risk assessments and observed that rollback must be ensured in case of failures in major changes.</p> <p>Upon enquiry, we have been informed that no major changes have been conducted during the declaration period. Thus, we have not been able to test the implementation and effectiveness.</p> <p>We have inspected that user are created with the lowest level of user rights.</p> <p>We have inspected that Abakion's developers have access to source code when there is a work-related need.</p>	<p>We have noted that a procedure for rollback has been implemented. However, we have not been able to comment on the implementation and effectiveness of the control, as no major changes have been conducted during the declaration period.</p> <p>No exceptions noted.</p>

A.14 System Acquisition, Development and Maintenance		
<b>Control objectives</b> ▶ To ensure that information security is prepared and implemented within information systems' development life cycle.		
Control Activity	Test performed by BDO	Result of test
<b>Separation of development, test, and production environments</b> <ul style="list-style-type: none"> <li>▶ Segregation between development and operations have been made.</li> <li>▶ Changes in functionalities are tested before they are put into production.</li> <li>▶ Development and test are done in the development environment which is separated from the test environment.</li> <li>▶ A version controlling system is used to register changes to the source code.</li> <li>▶ Development and test environment is separated.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected that functional separation between development and operation has been introduced. The environments are divided into production, test, and development environment.</p> <p>We have been informed that a sandbox of the production environment has been created and that it is a perfect copy of the production environment which is why the requirements to access it is the same as for the production environment.</p> <p>We have inspected Abakion's procedure for risk assessments and observed that major changes must be tested before they are put into production and the test must be done in an environment, which is separated from the production environment.</p> <p>Upon enquiry, we have been informed that no major changes have been conducted during the declaration period. Thus, we have not been able to test the implementation and effectiveness.</p> <p>We have observed that branches are used as version controlling system to register source code changes.</p>	<p>We have noted that a procedure for testing of major changes has been implemented. However, we have not been able to comment on the implementation and effectiveness of the control, as no major changes have been conducted during the declaration period.</p> <p>No exceptions noted.</p>
<b>Support assignments</b> <ul style="list-style-type: none"> <li>▶ Supporter's access and handling of personal data is solely performed based on a work-related need.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for support tasks.</p> <p>By random sampling, we have randomly inspected that supporters' access and handling of personal data is based on a work-related need.</p>	<p>No exceptions noted.</p>



**A.14 System Acquisition, Development and Maintenance****Control objectives**

► *To ensure that information security is prepared and implemented within information systems' development life cycle.*

Control Activity	Test performed by BDO	Result of test

A.15 Supplier relationships		
<b>Control Objective</b> ▶ To ensure protection of the organization's assets and the data that suppliers have access to. ▶ To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements.		
Control Activity	Test performed by BDO	Result of test
<b>Sub-service providers agreements and instruction</b>  ▶ All relevant suppliers have signed an NDA with Abakion and are familiar with the content of our information security manual.	We have made inquiries of relevant personnel at the service provider.  We have inspected that Abakion has entered into agreements with relevant suppliers and observed that they contain confidentiality obligations.	No exceptions noted.
<b>Control with service organisations</b>  ▶ Business procedures have been established to ensure supervision of Abakion's implemented controls in the form of obtaining an ISAE 3402 auditor's report.	We have made inquiries of relevant personnel at the service provider.  We have inspected that Abakion has carried out supervision of Microsoft by obtaining and reviewing the SOC1.  We have inspected that Abakion has carried out supervision of Continia Software by obtaining and reviewing ISAE 3402.  We have inspected that Abakion has carried out supervision of Global Mediator by obtaining and reviewing the ISO 27001 certificate and a questionnaire.  We have inspected that Abakion has carried out supervision of Atlassian by obtaining and reviewing the SOC 2.  We have inspected that Abakion has carried out supervision of Zendesk by obtaining and reviewing the ISO 27001 certificate.  We have inspected SOC 2 type II for the period 1 April 2023 to 31 March 2024 for Microsoft Azure.  We have obtained and inspected ISAE 3402 for the period 1 May 2023 to 30 April 2024 for Continia Software.	No exceptions noted.

## A.15 Supplier relationships

### Control Objective

- ▶ *To ensure protection of the organization's assets and the data that suppliers have access to.*
- ▶ *To maintain an agreed level of information security, data protection and delivery of services under the supplier agreements.*

Control Activity	Test performed by BDO	Result of test
	<p>We have obtained and inspected the ISO 27001 certificate for the period 3 July 2023 to 31 October 2025 and the questionnaire for Global Mediator.</p> <p>We have inspected SOC 2 type II for the period 1 October 2023 to 30 September 2024 for Atlassian.</p> <p>We have obtained and inspected the ISO 27001 certificate for the period 26 April 2024 to 14 April 2027 for Zendesk.</p>	

A.16: Information security incident management		
<b>Control Objective</b> ► To ensure a uniform and effective method of managing information security breaches including communication on security incidents and weaknesses.		
Control Activity	Test performed by BDO	Result of test
<b>Responsibilities and procedures</b> <ul style="list-style-type: none"> <li>► Management responsibilities and roles have been established in connection with breaches of information security.</li> <li>► The service provider has implemented a procedure for breaches of personal data security.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have observed that a procedure for breaches of information security has been implemented.</p> <p>We have observed that management responsibilities and roles in connection with breaches of information security has been defined in the relevant procedure.</p>	No exceptions noted.
<b>Registration of breaches of information security</b> <ul style="list-style-type: none"> <li>► The service provider registers data breaches in a data breach log.</li> <li>► The service provider has developed and implemented a procedure for experience collection after occurred data breaches.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's procedure for breaches of information security and observed that breaches of personal data security must be registered in the data breach log.</p> <p>We have inspected Abakion's data breach log and observed that no breaches of information security have been registered.</p> <p>We have inspected Abakions's procedure for breaches of information security and observed that a procedure for gathering experience in the event of breaches of information security is in place.</p> <p>Upon enquiry, we have been informed that there have been no breaches of information security. Thus, we have not been able to test the implementation and effectiveness.</p>	<p>We have noted that a procedure for reporting breaches of information security has been implemented. However, we have not been able to comment on the implementation and effectiveness of the control, as no breaches of information security occurred during the declaration period.</p> <p>No exceptions noted.</p>

A.18 Compliance		
<b>Control objectives</b> <ul style="list-style-type: none"> <li>▶ <i>To prevent violation of statutory and contract requirements in relation to information security and other security requirements.</i></li> <li>▶ <i>To ensure that information security is implemented and complied with in accordance with the organisation's policies and procedures.</i></li> </ul>		
Control Activity	Test performed by BDO	Result of test
<b>Identification of applicable legislation and contractual requirements</b> <ul style="list-style-type: none"> <li>▶ The service provider has identified all relevant statutory of requirements.</li> </ul>	<p>We have made inquiries of relevant personnel at the service provider.</p> <p>We have inspected Abakion's annual cycle and observed that all relevant statutory of requirements are identified.</p>	No exceptions noted.

**BDO STATSATORISERET  
REVISIONSAKTIESELSKAB**

**VESTRE RINGGADE 28  
8000 AARHUS C**

[www.bdo.dk](http://www.bdo.dk)

*BDO Statsautoriseret revisionsaktieselskab, a Danish limited liability company, is a member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO in Denmark employs more than 1,800 people and the world wide BDO network has about 120,000 partners and staff in more than 166 countries.*

*Copyright - BDO Statsautoriseret revisionsaktieselskab,  
cvr.nr. 20 22 26 70.*



# 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.”

## Kenneth Kryger Gram

CEO

På vegne af: Abakion A/S

Serienummer: c0f9b36d-f1b6-4a2f-894c-bd9ee1642d69

IP: 89.221.xxx.xxx

2025-02-06 14:02:07 UTC



## Nicolai Tobias Visti Pedersen

Partner , State Authorised Public Accountant

På vegne af: BDO Statsautoriseret revisionsaktiesels...

Serienummer: 096fe1fc-de80-4d55-8c69-fc2fb761227d

IP: 77.243.xxx.xxx

2025-02-06 14:10:33 UTC



## Mikkel Jon Larssen

BDO STATSAUTORISERET REVISIONSAKTIESELSKAB CVR: 20222670

Partner Head of Risk Assurance, CISA, CRISC

På vegne af: BDO Statsautoriseret revisionsaktiesels...

Serienummer: 51d312d9-1db3-4889-bb62-37e878df1fff

IP: 62.66.xxx.xxx

2025-02-06 14:25:46 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 med brug af certifikat og tidsstempel fra en kvalificeret tillidstjenesteudbyder.

### 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