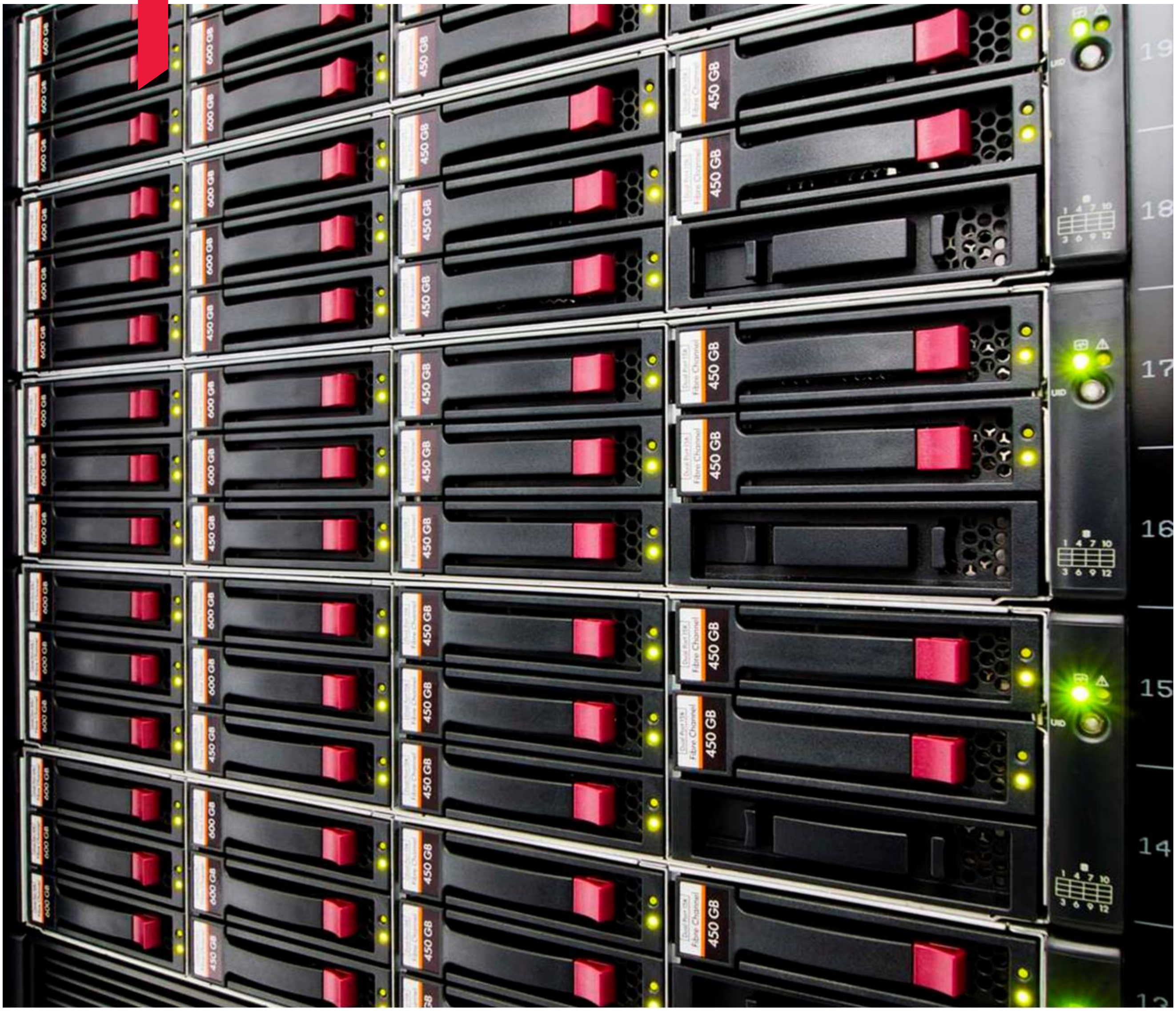

ABAKION A/S

INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT AT 18 JANUARY 2024 ON THE DESCRIPTION OF ABAKION A/S' DIGITAL BUSINESS SOLUTIONS CONTROLS AND THEIR DESIGN RELATING TO ABAKION A/S

CONTENTS

1. INDEPENDENT AUDITOR'S REPORT

INDEPENDENT AUDITOR'S ISAE 3402 ASSURANCE REPORT AT 18 JANUARY 2024 ON THE DESCRIPTION OF ABAKION DIGITAL BUSINESS SOLUTIONS AND RELATNG CONTROLS AND THEIR DESIGN.

To: The Management of 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 their design related to the control objectives stated in the description, at 18 January 2024.

We have not performed procedures regarding the operating effectiveness of the controls stated in the description, and accordingly, we do not express an opinion on this.

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 Control

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 and about the design of controls that relate to the control objectives set out in this description.

We have conducted our engagement in accordance with ISAE 3402 Assurance Engagements about controls with a service provider. That standard requires that we plan and perform our actions to obtain a high degree of assurance as to whether the description is fairly presented, and whether the controls are appropriately designed.

An assurance engagement to provide a statement about the description and design of controls at a service provider includes performing actions to obtain evidence of the information in the service provider's description and for the design of the controls. 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. An assurance assignment of this type further includes an assessment of the overall presentation of the description, the appropriateness of the control objectives set out herein and the appropriateness of the criteria specified and described by the service provider in section 2.

As described above, we have not performed procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, we do not express an opinion on this.

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 provider's description has been prepared to meet the common needs of a broad range of the service provider's customers and their accountants and therefore does not necessarily include all the aspects of Digital Business Solutions that each individual customer may consider important according to their particular environment. Furthermore, due to their nature, a service provider's controls may not prevent or detect all errors or omissions in the processing or reporting of transactions.

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 fairly presents the controls relating to Digital Business Solutions as designed and implemented at 18 January 2024, and

b. The controls related to the control objectives stated in the description were suitably designed and implemented at 18 January 2024.

Description of Test of Controls

The specific controls tested, and the 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, 25 January 2024

BDO Statsautoriseret Revisionsaktieselskab

Nicolai T. Visti	Mikkel Jon Larssen
Partner, State Authorised Public Accountant	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 customers who have used Digital Business Solutions, and who have a sufficient understanding to consider the description along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Abakion A/S uses sub-service providers. The relevant control measure(s) and associated controls of such sub-service providers are not included in 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 at 18 January 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. 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 implemented at 18 January 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.

Copenhagen, 25 January 2024

Abakion A/S

Kenneth Kryger Gran
CEO

3. ABAKION A/S' DESCRIPTION OF ABAKION 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. 160 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	IaaS	PaaS	SaaS	On Prem	LaaS
Risk assessment	• Risk assessment	x	x	x		x
A.5: Information security policies	• Information Security Policy • Review of information security policy	x	x	x	x	
A.6: Organisation of information security	• Roles and responsibilities • Segregation of duties • Mobil device policy • Remote workplaces and remote access to systems and data	x	x	x	x	
A.7: Human resource security	• Recruitment of employees • Training and instruction of employees who process personal data • Non-disclosure and confidentiality agreements • Resignation of employees	x	x	x	x	
A.8: Processing activities	• Inventory of assets	x	x	x	x	(x)
A.9: Access management	• User registration and deregistration • Allocation of user access • Management of privileged access rights • Review of user access rights	x	x	x	x	

ISO 27001	Control activities	IaaS	PaaS	SaaS	On Prem	LaaS
	- Use of Secret Authentication Information - Procedure for secure log-on - Logical access control					
A.10: Cryptography	- Policy for encryption - Administration of keys	x	x	x	(x)	
A.11: Physical and environmental security	- Policy for clean desk and desktop	x	x	x	x	
A.12: Operations security	- Maintaining system software - Antivirus program - Data backup - Logging in systems, databases, and networks, including logging of the use of personal data - Surveillance				(x)	
A.13: Communication security	- Network security - firewall - External communication connections				(x)	
A.14: Acquisition, development, and maintenance of systems	- Development and maintenance of systems - Information security in development and changes - Separation of development-, test and production environment - Support assignments	x	x	x	(x)	
A.15: Supplier relationships	- Sub service providers agreements and instructions - Control with service organisations	x	x	x	x	
A.16: Information security incident management	- Responsibilities and procedures - Registration of breaches of information security	x	x	x	x	
A.18: Compliance	- Identification of applicable legislation and contractual requirements	x	x	x	x	

(x) Advisory obligation.

DESCRIPTION OF CONTROL ENVIRONMENT

Description of Abakion A/S IT systems

Abakion has chosen to object to Microsoft as subcontractors 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 Abakions' 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 costumer 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 their immediate manager 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 the program "Easyinstall" 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.

4. CONTROL OBJECTIVES, CONTROL ACTIVITIES, TESTS AND RESULT 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 implementation 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 appropriately designed.

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

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 implemented at 18 January 2024.

Test procedures

Tests of the design of technical and organisational security measures and other controls, the implementation hereof was performed by inquiry, inspection, and observation.

Type	Description
Inquiry	Inquiries of relevant personnel at Abakion A/S have been performed for all significant control activities. 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.
Inspection	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. 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.
Observation	The use and existence of specific controls have been observed, including tests to ensure that the control has been implemented.

With respect to the services provided by Microsoft within Microsoft Azure, we have received a SOC 1 report for the period of 1 July 2022 to 30 June 2023 on technical and organisational security measures relating to Microsoft Azure.

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 organisational security measures and other controls for the period from 1 May 2022 to 30 April 2023.

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 organisational security measures and other controls for the period from 3 July 2023 to 31 Oktober 2025.

These sub-service provider’s relevant control objectives and related controls are not included in Abakion A/S’ description of Digital Business Solutions and relevant controls. Accordingly, we have solely assessed the report and tested the controls at Abakion A/S which ensures appropriate supervision of the operating effectiveness of the sub-service provider’s controls.

Result of test

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

An exception exists when:

- Technical and organisational security measures and other controls have not been designed or implemented to fulfil a control objective,
- Technical and organisational security measures and other controls related to a control objective are not suitably designed and implemented.

A.4 Risk Assessment

Control objectives

- *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
Risk assessment - A risk assessment of Abakion's solutions is carried out based on potential risks to the availability, confidentiality, and integrity of systems and data. - The vulnerability of systems and processes is assessed based on identified threats. - Risks are minimised based on the assessment of their probability, consequence, and derived implementation costs. - Risk assessments are updated regularly as needed, but at least once a year.	We have made inquiries of relevant personnel at the service provider. We inspected Abakion's risk assessment and associated procedure and observed that it has been updated in 2023, as well as based on data availability, probability and derived implementation costs based on the potential risks for data subjects' rights and freedom rights. We have inspected the risk assessment and observed that it covers identified vulnerabilities of systems and processes. 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.	No exceptions noted.

A.5 Security Policy

Control objectives

- *To provide guidelines for and supporting information security and data protection in accordance with business requirements and relevant laws and regulations.*

Control Activity	Test performed by BDO	Result of test
Policies for information security		
▶ The service provider has developed and implemented an information security policy. ▶ 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.	We have made inquiries of relevant personnel at the service provider. We inspected Abakion's information security policy and observed that it has been updated in 2023. 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.	No exceptions noted.
Review of information security policy		
▶ The service provider's information security policy is reviewed and updated at least once a year.	We have made inquiries of relevant personnel at the service provider. We inspected Abakion's information security policy and observed that it has been updated in 2023.	No exceptions noted.

A.6 Organisation of information security

Control objectives

- *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
Roles and responsibilities ▶ 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.
Segregation of duties ▶ 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.
Mobile device policy ▶ 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.
Remote workplaces and remote access to systems and data ▶ All mobile devices used in a work context must have antivirus installed and updated.	We have made inquiries of relevant personnel at the service provider.	No exceptions noted.

A.6 Organisation of information security

Control objectives

- *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
▶ Remote access to the service provider’s systems and data is via an encrypted VPN connection. ▶ Remote access must go via two-factor authentication.	By random sampling, we have inspected that antivirus is installed and updated. 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. 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. We have inspected that remote access goes via two-factor authentication.	

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
Recruitment of employees ▶ The service provider performs screening of potential employees before employment in the form of interviews and test cases. ▶ 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.	We have made inquiries of relevant personnel at the service provider. We have inspected the procedure for HR and for randomly selected employment observed that the procedure has been followed regarding screening of the employee. Regarding the background check we have by inquiry been informed that a background check was not performed as the randomly selected employee was known to Abakion, thus, a background check was deemed unnecessary.	No exceptions noted.
Training and instruction of employees in information security ▶ The service provider conducts instruction training of new employees in accordance with information security. ▶ The service provider carries out ongoing training of employees in accordance with information security and data protection as well as handling thereof.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's procedure for HR and observed that employees must receive training in data protection and information security. By random sampling we have inspected that new employees receive data protection and information security training as part of their onboarding. We have inspected that Abakion annually carries out training for all employees in data protection and information security.	No exceptions noted.
Non-disclosure and confidentiality agreements ▶ All employees working with confidential data – including personal data – have signed a confidentiality agreement.	We have made inquiries of relevant personnel at the service provider.	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
	We have inspected Abakion’s procedure for HR and observed that employees must sign an employment contract that contains a confidentiality agreement. We have inspected Abakion’s employment contract template and observed that it contains a confidentiality agreement. By random sampling, we have inspected that employees have signed an employment contract that contains a confidentiality agreement.	
Resignation of employees - The service provider has prepared and implemented a procedure for offboarding employees. - Upon resignation, the employee is informed that the signed confidentiality agreement is still valid.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's Procedure for HR and observed that it contains a procedure for resignation. We have inspected Abakion’’s resignation template. By random sampling, we have inspected that resigning employees have returned assets and user access is terminated. We have inspected Abakion’s Procedure for HR and observed that resigning employees are informed that the signed confidentiality agreement is still valid. By random sampling, we have inspected that employees are informed that the signed confidentiality agreement is still valid upon resignation.	No exceptions noted.

A.8 Asset management

Control Objective

- *To identify the organisation's assets and define appropriate responsibilities for its protection.*

Control Activity	Test performed by BDO	Result of test
Inventory of assets ▶ 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 the service provider's inventory of assets list in relation to information and information processing facilities.	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
User registration and deregistration ▶ The service provider has implemented a used administration procedure that ensures that user creations and closures follow a controlled process and that all user creations are authorised.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's procedure for access management and observed that creations and closures follow the procedure. If a customer wants user-specific access, the customer himself is responsible for this, as a user is granted access from Abakion to the relevant customer's environment, after which the customer sets up the user in their environment. By random sampling, we have inspected that an employee is granted access based on a work-related need. By random sampling, we have inspected that an employee's access is terminated upon resignation.	No exceptions noted.
Allocation of user access ▶ The service provider has a record of users with access to systems with personal information. ▶ User rights are allocated based on a work-related-need.	We have made inquiries of relevant personnel at the service provider. 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. By random sampling, we have inspected that an employee is granted access based on a work-related need.	No exceptions noted.
Management of privileged access rights		

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
▶ Privileged accounts (administrative rights) to systems are granted based on a work-related need.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's procedure for access management. Upon enquiry, we been informed that all employees with access to customers' environments have "administrative rights", however, this has been deemed necessary for the employees to be able to perform their tasks.	No exceptions noted.
Review of user access rights ▶ Users and user rights are reviewed annually.	We have made inquiries of relevant personnel at the service provider. We have inspected that Abakion reviews users and user rights annually.	No exceptions noted.
Use of secret authentication information ▶ The service provider has established rules for password requirements, which must be followed by all employees as well as external consultants.	We have made inquiries of relevant personnel at the service provider. We have inspected the procedure for use of passwords and observed an excerpt of the AD password policy from which we could observe that password requirements are enforced on all employees and external consultants.	No exceptions noted.
Procedure for secure log-on		

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
▶ The service provider has established logical access control for systems with personal data, including two-factor authentication.	We have made inquiries of relevant personnel at the service provider. We have inspected that Abakion has established logical access control for systems with two-factor authentication.	No exceptions noted.
Logical access control ▶ A log is kept for all accesses to systems and data.	We have made inquiries of relevant personnel at the service provider. We have inspected that all access to systems and data is logged and observed that the data logged is maintained by Microsoft.	We have found that the retention period of the log is too short. No further exceptions noted.

A.10 Cryptography

Control objectives

- *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
Policy for the use of cryptography - The service provider has implemented an encryption policy for encrypting personal data. The policy defines the strength and protocol of encryption. - Portable media is encrypted. - Encryption is used for the transmission of confidential and sensitive personal information via the internet and e-mail.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's encryption policy and observed that personal data must be encrypted. We have inspected Abakion's encryption policy and observed that portable media with personal data must be encrypted. By random sampling, we have inspected that portable media are encrypted. We have inspected the Abakion''s encryption policy and observed that e-mails must be encrypted if confidential or sensitive personal data is transmitted.	No exceptions noted.
Administration of keys - The encryption keys are stored in a location other than where encrypted data is stored.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's policy for encryption and observed that keys must be stored in another location. We have inspected that encryption keys are stored in a location that is different from where encrypted data is stored.	No exceptions noted.

A.11 Physical and environmental security

Control objectives

- *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
Policy for clean desk and desktop - 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 workstations must be locked when leaving the office.	No exceptions noted.

A.12 Operation procedures

Control objectives

- *To ensure correct and secure operation of information processing facilities.*
- *To ensure that information and information processing facilities are protected against malware.*
- *To protect against loss of data.*
- *To register incidents and provide evidence.*
- *To ensure the integrity of operating systems.*
- *To prevent the exploitation of technical vulnerabilities.*
- *To minimise the effect of audit activities on operation systems.*

Control Activity	Test performed by BDO	Result of test
Maintaining system software ▶ The service provider has implemented a process for updating system software with regards to ensuring the systems' availability and security. ▶ Operating systems software on workstations are regularly updated.	We have made inquiries of relevant personnel at the service provider. 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. By random sampling, we have inspected that Abakion continuously updates system software on workstations. By random sampling, we have inspected that Abakion continuously updates system software on servers.	No exceptions noted.
Antivirus program ▶ Antivirus software is installed on all servers and workplace stations. ▶ Antivirus software is constantly updated and updated with the latest version.	We have made inquiries of relevant personnel at the service provider. By random sampling, we have inspected that antivirus is installed and continuously updated on the computer. By random sampling, we have inspected that antivirus is installed and continuously updated on servers.	No exceptions noted.

A.12 Operation procedures

Control objectives

- *To ensure correct and secure operation of information processing facilities.*
- *To ensure that information and information processing facilities are protected against malware.*
- *To protect against loss of data.*
- *To register incidents and provide evidence.*
- *To ensure the integrity of operating systems.*
- *To prevent the exploitation of technical vulnerabilities.*
- *To minimise the effect of audit activities on operation systems.*

Control Activity	Test performed by BDO	Result of test
Data backup ▶ Systems and data are backed up daily.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's procedure for backup and observed that backups are carried out daily. We have inspected that backups are carried out daily. By random sampling, we have inspected that failed backups are rectified.	No exceptions noted.
Logging in to systems, databases, and networks, including logging of the use of personal data ▶ All successful and unsuccessful attempts to access the service provider's systems and data are logged.	We have made inquiries of relevant personnel at the service provider. We have inspected that all successful and unsuccessful attempts to access Abakion's systems and data are logged.	No exceptions noted.
Surveillance ▶ The service provider has established a surveillance system of the production environment surveillance e.g., uptime, performance, and capacity. ▶ The service provider is notified regarding identified alarms and there is followed up on such.	We have made inquiries of relevant personnel at the service provider. We have inspected that Abakion has established a monitoring system.	No exceptions noted.

A.12 Operation procedures

Control objectives

- *To ensure correct and secure operation of information processing facilities.*
- *To ensure that information and information processing facilities are protected against malware.*
- *To protect against loss of data.*
- *To register incidents and provide evidence.*
- *To ensure the integrity of operating systems.*
- *To prevent the exploitation of technical vulnerabilities.*
- *To minimise the effect of audit activities on operation systems.*

Control Activity	Test performed by BDO	Result of test
	We have inspected that Abakion follows up on unidentified alarms.	

A.13 Communications Security

Control objectives

- *To ensure protection of information in networks and of supporting information processing facilities.*
- *To maintain information security at internal transmission in an organisation and to an external entity.*

Control Activity	Test performed by BDO	Result of test
Network security - Network topology is structured according to best practise so that servers that manage the application cannot be reached directly from the internet. - The service provider's network is separated so the internal server cannot communicate directly with the internet. - The service provider uses well-known network technologies and mechanisms to protect the internal network.	We have made inquiries of relevant personnel at the service provider. We have observed that VPN, Gateway, and two-factor authentication are used to protect servers. We have inspected Abakions physical network and observed that Abakions network is separated so internal servers cannot communicate directly with the internet. We have observed that firewalls have been set-up on Abakion's VLAN.	No exceptions noted.
Firewall - The service provider only uses services/ports which are needed. - Firewalls are configurated and validated periodically an as needed to ensure that services/ports only are opened as they are needed.	We have made inquiries of relevant personnel at the service provider. We have inspected relevant documentation and observed that Abakion only uses services/ports which are needed. We have inspected that firewalls are configurated and observed that firewalls are validated periodically and as needed.	No exceptions noted.
External communication connections - External connection to systems and databases, which are used to process personal data, occurs through secure firewall and VPN.	We have made inquiries of relevant personnel at the service provider. 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.	No exceptions noted.

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
Development and maintenance of systems ▶ The service provider works based on the relevant principals in development and maintenance assignments. ▶ Risk evaluations of systems changes are done, to ensure data protection by design.	We have made inquiries of relevant personnel at the service provider. We have inspected that Abakion works based on security-by-design principles in development and maintenance assignments.	We have established that the data processor does not carry out risk assessments of system changes, but this is expected to be incorporated in the future. No exceptions noted.
Information security in development and changes ▶ The service provider works based on the principles of security-by-design in development and maintenance assignments. ▶ Rollback is ensured through version-controlled source codes in case of failures in the production environment. ▶ Users are generally created with lowest level of user rights. ▶ Solely the service provider's developers and project leaders with a work-related need have access to the source codes.	We have made inquiries of relevant personnel at the service provider. We have inspected that Abakion works based on security-by-design principles in development and maintenance assignments. By random sampling we have inspected that the rollback plan has been implemented in the event of errors in the production environment We have inspected that user are created with the lowest level of user rights. We have inspected that Abakions's developers have access to source code when there is a work-related need.	No exceptions noted.
Separation of development, test, and production environments ▶ Segregation between development and operations have been made. ▶ Changes in functionalities are tested before they are put into production. ▶ Development and test are done in the development environment which is separated from the test environment.	We have made inquiries of relevant personnel at the service provider. We have inspected that functional separation between development and operation has been introduced. The environments are divided into production, test, and development environment.	No exceptions noted.

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 version controlling system is used to register changes to the source code. ▶ Development and test environment is separated.	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. By random sampling, we have inspected that changes are tested before they are put into production. By random sampling, we have inspected that changes are tested in development environments that are separate from production systems before they are put into operation. We have observed that branches are used as version controlling system to register source code changes.	
Support assignments ▶ Supporter’s access and handling of personal data is solely performed based on a work-related need.	We have made inquiries of relevant personnel at the service provider. We have inspected Abakion's procedure for support tasks. By random sampling, we have randomly inspected that supporters' access and handling of personal data is based on a work-related need.	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
Sub-service providers agreements and instruction 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.
Control with service organisations 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 SOC 1 as well as the Bridge Letter. We have inspected that Abakion has carried out supervision of Continia Software by obtaining and ISAE 3402. We have inspected that Abakion has carried out supervision of Global Mediator by obtaining and reviewing the ISO 27001 certificate as well as an additional follow-up questionnaire. We have inspected that Abakion has not carried out supervision of Evanate, but that they will later carry out a supervision. We have inspected SOC 2 type I for the period 1 July 2022 to 30 June 2023 for Microsoft Azure. We have obtained and inspected ISAE 3402 for the period 1 May 2022 to 30 April 2023 for Continia Software. We have obtained and inspected the ISO 27001 certificate for the period 3 July 2023 to 31 October 2025 for Global Mediator.	We have found that Abakion has not carried out sufficient supervision of Enavate. No further exceptions noted.

A.16: Information security incident management

Control Objective

- *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
Responsibilities and procedures		
▶ Management responsibilities and roles have been established in connection with breaches of information security. ▶ The service provider has implemented a procedure for breaches of personal data security.	We have made inquiries of relevant personnel at the service provider. We have observed that a procedure for breaches of information security has been implemented. We have observed that management responsibilities and roles in connection with breaches of personal data security has been defined in the relevant procedure.	No exceptions noted.
Registration of breaches of information security		
▶ The service provider registers data breaches in a data breach log. ▶ The service provider has developed and implemented a procedure for experience collection after occurred data breaches.	We have made inquiries of relevant personnel at the service provider. 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. We have inspected Abakion's data breach log and observed that no breaches of information security have been registered. 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. 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.	No exceptions noted.

A.18 Compliance

Control objectives

- *To prevent violation of statutory and contract requirements in relation to information security and other security requirements.*
- *To ensure that information security is implemented and complied with in accordance with the organisation's policies and procedures.*

Control Activity	Test performed by BDO	Result of test
Identification of applicable legislation and contractual requirements		
The service provider has identified all relevant statutory of requirements.	We have made inquiries of relevant personnel at the service provider. We have inquired documentation verifying that the service provider is aware of relevant legislation, and we have observed that relevant legislation is followed.	No exceptions noted.

BDO STATSAUTORISERET
REVISIONSAKTIESELSKAB

HAVNEHOLMEN 29
1561 KØBENHAVN V

CVR NO. 20 22 26 70

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 almost 1,700 people and the worldwide BDO network has more than 111,000 partners and staff in 164 countries.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, 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: 109.56.xxx.xxx
2024-01-27 13:52:31 UTC
MitID ✓

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
2024-01-28 09:31:49 UTC
MitID ✓

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
2024-01-28 15:12:57 UTC
MitID ✓

Penneo dokumentnøgle: 6HQSE-V3JMP-10ANC-7VY23-V4JG2-AJGWP