www.pwc.dk

# *Visma Acubiz A/S*

## Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 May 2023 to 31 December 2023 in relation to Acubiz Solution standard operating platform

*March 2024*

# Contents

# 1 Management's statement

The accompanying description has been prepared for customers who have used Acubiz Solution standard operating platform and their auditors who have a sufficient understanding to consider the description, along with other information including information about controls operated by customers themselves, when assessing the risks of material misstatements in customers' financial statements.

Visma Acubiz A/S uses Visma IT and Progressive A/S as a subservice supplier of infrastructure operation (IaaS). This report uses the carve-out method and does not comprise control objectives and related controls that Visma IT and Progressive A/S performs for Visma Acubiz A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

Visma Acubiz A/S confirms that:

a) The accompanying description in section 3 fairly presents the Visma Acubiz A/S' services that has processed customers' transactions throughout the period from 1 May 2023 to 31 December 2023. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to Visma Acubiz A/S' services were designed and implemented, including:

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

   (ii) Includes relevant details of changes to IT general controls in relation to Visma Acubiz A/S' services during the period from 1 May 2023 to 31 December 2023

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 May 2023 to 31 December 2023. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 May 2023 to 31 December 2023.

Copenhagen, 22 March 2024
**Visma Acubiz A/S**

Henrik Malling

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

**Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 May 2023 to 31 December 2023 in relation to Acubiz Solution standard operating platform**

To: Visma Acubiz A/S, customers and customers' auditor

**Scope**

We have been engaged to provide assurance about Visma Acubiz A/S' description in section 3 of its IT general controls in relation to Visma Acubiz A/S' services which has processed customers' transactions throughout the period from 1 May 2023 to 31 December 2023 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Visma Acubiz A/S uses Visma IT and Progressive A/S as a subservice supplier of infrastructure operation (IaaS). This report uses the carve-out method and does not comprise control objectives and related controls that Visma IT and Progressive A/S performs for Visma Acubiz A/S.

Some of the control objectives stated in Visma Acubiz A/S' description in section 3 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with Visma Acubiz A/S' controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

**Visma Acubiz A/S' responsibilities**

Visma Acubiz A/S is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

**Service auditor's independence and quality control**

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

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

**Service auditor's responsibilities**

Our responsibility is to express an opinion on Visma Acubiz's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its development and hosting services and about the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by Visma Acubiz A/S in the Management's statement section.

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**

Visma Acubiz's description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any 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 auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to Visma Acubiz A/S' services were designed and implemented throughout the period from 1 May 2023 to 31 December 2023.

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 May 2023 to 31 December 2023; 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 May 1 2023 to 31 December 2023.

**Description of test of controls**

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

**Intended users and purpose**

This report and the description of tests of controls in section 4 are intended only for customers who have used Visma Acubiz's service and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Aarhus, 22 March 2024
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

# 3 Visma Acubiz A/S' description of IT general controls relating to Acubiz Solution standard operating platform

## 3.1 Introduction

This report has been prepared in accordance with:

**I**nternational **S**tandard on **A**ssurance **E**ngagements (ISAE) 3402:
'Assurance Reports on Controls at a Service Organization'

The objective of this report is to provide information to auditors of user organizations on Visma Acubiz provided services and internal controls related to the services in scope.

The report is intended to focus only on the controls within Visma Acubiz that may be relevant to the respective control environment of each user organization.

This section provides an overview of all identified control objectives.

The report on services, related control objectives and controls placed in operation and tests of their operating effectiveness is intended to provide interested parties with sufficient information to understand the transaction flows in order for the interested parties to rely on certain controls in place within Visma Acubiz.

The examination has been performed in accordance with ISAE 3402. Each user organization is responsible for evaluating this information in relation to the internal control structure in place at their organization in order to assess the total internal control structure.

If an effective user organization's internal control structure is not in place, the related Visma Acubiz internal control structure may not compensate for such weaknesses.

## 3.2 Overview and description of extensive services

Visma Acubiz was established in 1997 and was based in Birkerød. In December 2021 Acubiz was bought by Visma and became a legal entity in Visma. Visma Acubiz moved to Visma's HQ in Copenhagen in September 2022. Visma Acubiz provides the cloud-based travel expense solution ACUBIZ SOLUTION which is an Expense Management Service.

## 3.3 Audit scope

This Service Auditor Report covers the following standard operating system from Visma Acubiz:

Acubiz Solution (Standard Version 7)

This report includes:

Operations monitoring, including handling of security:

- Information security
- Organization of information security
- Human Resource security

- Asset Management
- Access control
- Physical and environmental security
- Operations security
- Communication security
- System acquisition
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management

The services in scope are described in the following paragraphs.

### 3.3.1 Acubiz Solution

Acubiz Solution (Standard version 7) is a web-based travel expense service, streamlining the procedures for handling travelling expenses and other employee expenses. It is provided as a hosted solution and is available to users, super users and administrators via a web interface (Internet Explorer Version 11 or newer version).

Acubiz Solution basically consists of an automatic workflow, where e-transactions and cash expenses are automatically placed with the employee, who with a few clicks may create a travel expense report, enter costs and send the travel expense report for approval and export. Thereafter, the file is ready for import into the company's financial management systems.


Acubiz Solution (Standard Acubiz) covers the following areas/functionalities:

| Function | Description |
|---|---|
| **Credit card integration** | Automatic importing of credit card transactions |
| **Travel account integration** | Automatic importing of travel card transactions |
| **Cash outlay** | Reimbursement of cash outlay |
| **Advances/return advances** | Registration of cash advances/return advances |

| | |
|---|---|
| **Allowance** | Calculation, reporting and reimbursement of daily allowance |
| **Travel orders** | Process for prior approval of travel |
| **Export** | Option of exporting data for subsequent entry in the finance system and/or payroll system |

Visma Acubiz has full control of the development and distribution of this solution. We deliver Acubiz Solution as SAAS, we perform system development of the standard solution, we offer implementation and support to our customers, both public and private, within a wide range of businesses, including without limitation:

- Pharmaceuticals
- Financial institutions
- Lawyers
- Auditors
- Transportation and logistics

### *3.3.2 Data handling*

Visma Acubiz is responsible for the daily (Monday-Sunday) loading of electronic transactions (supplied from data suppliers to Acubiz servers) into the customer's application.

Visma Acubiz is responsible solely for the transport of the transactions and not for the contents of individual data files.

In order to ensure stable operation and to maintain the confidentiality, reliability and accessibility of Acubiz Solution systems and data, Visma Acubiz has planned processes and controls, which protect and cover the customer's business requirements.

## *3.4 Description of internal controls at entity level*

### *3.4.1 Internal control elements*

#### 3.4.1.1 Control environment

Control environment includes organisation structure, governance, policies and procedures and defines the organisation's general view on internal controls.

#### 3.4.1.2 Control activities

Control activities include policies and processes in order to ensure that decisions and measures by the management are implemented in the entity.

#### 3.4.1.3 Information and communication

This item includes formal, informal and automated systems, which ensure identification, capture and exchange of information so that the employees of the user organization may carry out their work satisfactorily with respect to performance as well as time.

#### 3.4.1.4 Monitoring

This item includes processes to ensure that the quality of the controls is maintained and complies with the quality targets over time.

#### 3.4.1.5 Risk assessment

Method for identification and analysis of risks, which may affect Acubiz's goals and activities. It provides a basis for counteracting and handling these risks.

## 3.4.2 Control environment

The elements in Acubiz's internal control include controls, which may have a radical and permanent effect on Acubiz as a whole or on processes, applications, and transactions patterns. Certain control elements relate to the organization while others relate to specific procedures or applications.

### 3.4.2.1 Organizational structure

Visma Acubiz's legal owners are Visma Denmark Holding. Acubiz A/S Board consist of 3 Visma employees, of which 1 is Chairman of the Board and further 2 persons are Board Members.

Visma Acubiz's organization is divided into 9 main areas: "Acubiz Board", "Directors and Management"; "Product and Development", "Operational Excellence and IT-Operation, "Customer Relations", "Marketing and Communications"-" Sales" – "Partnerships" and "Finance and Admin", which all are grouped under a common management with common administration.,

| | |
|---|---|
| Acubiz Board | Strategy and Business development |
| Directors and Management | Information Security Board and Product Board |
| Product and Development | Standard EMS and customization, testing and upgrading of customer's solution |
| Operational Excellence and IT-Operation IT | Hosting, Edi, IT administration, internal and customer-related operations |
| Customer Relations | Implementation and training, Service desk and support functions |
| Marketing and Communication | Digital marketing, Brand and Communication |
| Sales | Sales and Key account |
| Partnerships | Sales and 3rd partners (products) |
| Finance and Admin | Procurement, bookkeeping and other administrative tasks |

### 3.4.2.2 Governance

The management of Visma Acubiz consists of Acubiz's Managing Director, the Development Director, the Customer Relations Director, the Finance Director and Commercial Director.

The management is generally responsible for preparing policies and ensuring that these are implemented in the organization and that they are supported by the necessary procedures and controls and that the employees understand, accept and comply with the policies as well as the underlying procedures and controls. The practical tasks in connection with the implementation and support may be delegated to the management group or the rest of the organization but the general responsibility remains with the management.

The management establishes responsibilities and authorizations for the individual groups or employees in the organization and determines approval hierarchies as well as rules and procedures for reporting.

### 3.4.2.3 Policies and procedures

The executive management is also responsible for HR policies and practice regarding employment, information, training, evaluation, promotion and compensation of employees. However, the HR procedures before employment (such as recruiting, 1st interviews etc.) is outsourced to Visma Enterprise HR.

Visma Acubiz, being part of the Visma Group, also join Visma Group policies and support and maintain the desired values and attitudes of Visma. Which, among other things, describes the importance of the individual employee always maintains a high degree of integrity and acting in accordance with the Group's values and the current legislation. This includes all employees as part of the employment signs an NDA.

## *3.4.3 Information and communication*

Information and communication are an integral part of Visma Acubiz's internal control system. It covers the processes, which concern identification, collection and exchange of information, form and time frames necessary to manage and control the company's operation. Visma Acubiz identifies processes and reports information through various information systems and dialogue with customers, employees, and other external stakeholders.

### 3.4.3.1 Information systems

Visma Acubiz's information systems are grouped into different applications:

- TAW: The Acubiz Way holds description of Acubiz's procedures and processes.
- BITE: This database holds customers' and their database (s) master data.
- 360: This database holds the registration of the chosen services for each customer.
- STAT: Is Acubiz's statistical tool.
- PCR: Is the old Product Change Request database which holds description and overview of customers' change requests.
- Visma Google Drive holds 3402 control procedures and processes.
- Visma Tech Hubs holds Information Security Management System, Visma Cloud Delivery Model, Quality Management System, Confluence,
- Jira, Project Management Tool for all new Product Change Requests
- Slack, internal company-based communication

At the start of employment, it is assessed to which applications the new employee should have access based on his/her work tasks. Application access is thus in line with the job function and will therefore be reassessed in the event of changes to the employment.

## *3.4.4 Monitoring*

Acubiz continuously assesses the overall set of controls to secure they sufficiently fulfil the requirements, which we, our customers or the legislation set to us.

### 3.4.4.1 Risk assessment

Risk assessment is a critical point in Visma Acubiz's internal control system for handling and continuously assessing risks. The purpose is to identify and classify the risks that may affect the organization's ability to function, see Visma Acubiz's obligations according to Visma Acubiz's General Terms. Visma Acubiz's management is aware of the fact that risks must be reported and treated separately in order to counteract and deal with them, see the stipulated framework.

The challenges faced by Visma Acubiz are therefore assessed and controlled continuously, based upon the result of the risk assessment. If a given risk is identified and found to be significant, separate monitoring is initiated to update the relevant documents, processes and business procedures to ensure mitigation (risk reduction) in relation to the business.

Information security risk assessments are conducted in accordance with recommendations from the Danish Data Protection Agency (Datatilsynet) and ISO/IEC 27001.

Risk assessment model:

| Likelihood | Risk levels | | | | |
|---|---|---|---|---|---|
| 4 - Almost certain | 4 | 8 | 12 | 16 | |
| 3 - Likely | 3 | 6 | 9 | 12 | |
| 2 - Possible | 2 | 4 | 6 | 8 | |
| 1 - Rare | 1 | 2 | 3 | 4 | |
| | 1 - Minor | 2 - Moderate | 3 - Major | 4 - Severe | Impact |

### 3.4.5 Major Changes during Q2 2023– Q4 2023

Certain activities have already been completed. Such as the Key elements in the long-term strategy which has been defined and *enhancing information security*, centered around people, process, partners and products (4 P's). For this purpose, Visma is providing its portfolio companies with a comprehensive framework for working with information security, this includes Group policies. Policies at Group level are mandatory and is the minimum level of security.

The latest change took place during Q3 and Q4 2023, where Acubiz changed Subprocessor (Hosting) from Progressive A/S to Visma IT A/S.

## 3.5 Description of operations monitoring, including handling of security processes

### 3.5.1 Information Security policy

Visma Acubiz's information security policy

Based on risk assessment, a set of information security policies has been established and approved by management (ISB) The policies have been published and communicated to employees and relevant external parties. The policies are reviewed on an annual basis or when required due to significant changes to ensure their continued appropriateness, adequacy, and effectiveness.

(Control no.: A5.1)

### 3.5.2 Organization of information security

Internal organization.

Visma Acubiz's management has established an Information Security Board, where roles and responsibilities are set out. The objective is to manage, to initiate, to control the implementation and operation of information and security within the organization.

Conflicting duties between critical functions of Visma Acubiz and areas of responsibility have been segregated. This includes segregation of duties internally between development, test and production with proper consideration of the use of sub service organizations.

(Control no.: 6.1)

### 3.5.3 Human resource security

Prior to employment, Visma Acubiz ensures that employees and external consultants understand their responsibilities and that they are suitable for the roles for which they are considered. This includes screening of criminal records and contractual agreements (including non-disclosure agreement) with employees and external consultants stating their and the organization's information's security responsibilities.

During Employment, Visma Acubiz ensures that employees and external consultants are aware of their information security responsibilities. This includes information's security awareness, training and education.

(Control no.: A7.1, A7.2)

### 3.5.4 Asset management

Visma Acubiz has identified organizational assets and defined appropriate protection responsibilities. An asset inventory has been drawn up and is maintained, including acceptable use of information and assets like return, transfer, disposal. etc.

Visma Acubiz ensures that information receives an appropriate level of protection in accordance with its importance to the organization. This includes classification of information in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification. Procedures for handling assets have been established and implemented.

Procedures for physical media transfer and for disposal of media have been established and implemented to prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.

(Control no.: A8.1, A8.2)

### 3.5.5 Access control

Visma Acubiz ensures that access to information and information processing facilities is limited. An access control policy, based on business and information security requirements has been established and documented and is reviewed on a regular basis. Users are only provided with access to services that they have been specifically authorized to use.

Visma Acubiz ensures authorized user access to prevent unauthorized access to systems and services. A process for user registration, de-registration and user access provisioning has been established and implemented. Privileged access rights as domain administrators are restricted and controlled. User access rights to restricted information are reviewed at regular intervals

The access rights to information and information processing facilities are removed upon termination of employment.

Visma Acubiz employees are accountable for safeguarding their authentication information. Users are instructed to follow the organization's practices in the use of secret authentication information.

(Control no.: A9.1, A9.2)

### 3.5.6 Physical and environmental security

Visma Acubiz, following Visma Group policy, ensures that unauthorized access to the organization's information and information processing facilities is prevented. Security perimeters are defined, and offices, rooms and facilities are secured by physical entry controls.

A policy regarding clear desk, clear screen and removable storage media has been established and implemented

(Control no.: A11.1)

### 3.5.7 Operation security

Visma Acubiz ensures correct and secure operation of information processing facilities. A policy on operational procedures has been established, and a change management workflow has been implemented to ensure the control of changes to the production environment. Development, test and production environments are separated, and changes to the production environment must be planned and tested.

Visma Acubiz ensures that information is protected against malware. Visma Acubiz has implemented and communicated an acceptable use policy.

Visma Acubiz ensures the protection against loss of data. Back-up and back-up restore tests are performed on a regular basis.

Visma Acubiz minimizes the risk of exploitation of technical vulnerabilities by an effective patch procedure, penetration testing and continuous vulnerability scanning will be according to a defined schedule.

(Control no.: A12.1, A12.2, A12.4, A12.6)

### 3.5.8 Communications security

Visma Acubiz ensures the protection of information in networks and its supporting information processing facilities. Network are managed and controlled, and groups of information services and users are segregated on networks.

(Control no.: A13.1)

### 3.5.9 System Acquisition development and maintenance

Visma Acubiz ensures that information systems are designed and implemented according to the systems development and security process, which ensures a structured and well-controlled environment.

We have recently adapted the Visma de facto task management tool (currently Jira), and a limited set of users has been granted access to add items to the backlog. Jira allows for documentation of who has access and what each user does. To ensure data secrecy, Jira uses industry standard AES 256 encryption. Generally, the development task initiated is based upon overall Product Board decisions. Furthermore, peer reviews are in place before testing code.

The process is initiated by the Product Board, which is responsible for business development, including decisions on the development of new functionalities.

Development and security process:

IDEAS

- We have several channels for new ideas and the formalized ones are:
- Mailbox for wishes from customers (idea.acubiz@visma.com)
- Slack channel for bug reporting #acubiz-productbugs
- Slack channel for product suggestions #acubiz-productsuggestions
- The Product Board

PRIORITY

Priorities is done in the Product Board meetings and can also be handled in the slack channel.

DEVELOPMENT
Approved overall tasks are added to the development Jira project, and from there it follows our standard development process

TEST
All implementations are finalized with a manual test

3D TEST
Before every versioned release, a so-called 3D test is performed. It is a structured test, that ensures the complete system still works as expected (14.2.3).

RELEASE
We release to new and pilot customers first, and if successful - mass released in batches of 50-100 customers is done gradually.

The adopted additions are described in Jira, where the development is monitored with respect to code review, test course and status.

When the number of planned functions has been developed, a new version is then created to be ready for 3-D testing. After successful tests, all customers are upgraded after approval by the Product Board.

Updating of customer databases includes a process where it is tested that new functionalities in the standard can be implemented without problems.

*Minor roll-out*
Minor releases may occur in the period between major releases, where individual sprints containing a new feature are closed/saved as new version, and where this version is made available to one or more customers, which have just requested the feature developed in this sprint. New customers established in the period between major releases may also be offered to get this version.

Visma Acubiz ensures the protection of data used for testing. An approach to testing as well as strategies and design techniques for testing have been established.

Visma Acubiz's internal control has the overall responsibility for ensuring that periodic controls are carried out.

(Control no.: A14.2)

## *3.5.10 Supplier relationships*

Visma Acubiz utilizes subservice organisations for certain purposes.

Below is a description of the most significant subservice organization handled by supplier relationship management

- Visma IT
  Acubiz has outsourced part of its operation to external hosting partner. Acubiz receives an Independent Service Auditor's Report covering the operations delivered by the subservice provider. The reports are prepared in accordance with ISAE3402 and ISAE3000 Visma IT are our IaaS service provider for handling and storing all central IT equipment

Visma Acubiz maintains an agreed level of information security and service delivery in line with supplier agreements by monitoring, reviewing and auditing supplier service delivery on a regular basis. Visma Acubiz review the supplier's fulfillment of the information security requirements
(Control no.: A15.2)

### 3.5.11 Information security incident management

Visma Acubiz ensures a consistent and effective approach to the management of information security or privacy incidents, including communication on security or privacy events and weaknesses. A process for information security or privacy events or weaknesses has been established and implemented. Reported information security or privacy events and weaknesses are reviewed and classified on a regular basis.

(Control no.: A16.1)

### 3.5.12 Information security aspects of business continuity management

A business impact assessment has been performed.

A business Continuity Management policy has been established.

Business Continuity plans and action cards have been established and implemented and will, together with the Continuity Management, be verified on a regular basis

(Control no.: A17.1)

## 3.6 Complementary user entity controls

Visma Acubiz services are designed on the assumption that certain controls would be implemented by user organizations.

In certain situations, the application of specific controls of the customer organizations are necessary to achieve certain control objectives included in this report.

The list below describes additional controls that should be in operation in customer organizations to complement the controls at Acubiz. Customer auditors should consider and ensure that the following controls have been implemented and carried out in the customer organizations:

- Visma Acubiz's customers are responsible for validation of their data input in Acubiz Solution.
- Visma Acubiz's customers carry out a physical access control on their own premises.
- Visma Acubiz's customer users have logical access control (login).
- Visma Acubiz's customers are responsible for their own creation and closing of users. They are also responsible for ensuring that user rights are granted based on a work-related need.
- Visma Acubiz's customers are responsible for testing that the specific customization is working as required.
- Visma Acubiz's customers are responsible for their own changes/updates of mileage, currency and/or allowance rates, if these are agreed to be performed by the customer. Customers outside Scandinavia, Germany and the UK are responsible for controlling that the rates/rules are in sync with their specific country rules.

The list does not represent, and should not be considered, a comprehensive listing of the control policies and procedures which would provide a basis for the assertions underlying clients' financial statements.

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

**5.1 Management direction for information security**

**Control objective:** Management must establish a set of policies for information security. The policies must be reviewed and approved regularly and published and communicated to relevant parties.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **5.1.1 Policies for information security**<br>*A set of policies for information security should be defined, approved by Management, published and communicated to employees and relevant external parties.*<br>A set of policies for information security are defined, approved by Management, published and communicated to employees and relevant external parties. | By inspection, we have observed that a Management-approved and up-to-date security policy is in place.<br>By inspection, we have verified that the security policy is reviewed at least once a year.<br>By inspection, we have verified that the information security policies are communicated to employees and relevant parties. | No exceptions noted. |
| **5.1.2 Review of policies for information security**<br>*The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.*<br>The policies for information security are reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness. | By inspection, we have observed that the policies for information security are reviewed at planned intervals or in connection with significant changes. | No exceptions noted. |

**6.1 Organisation of information security**

**Control objective:** Management must establish an organisation in which roles and responsibilities regarding information security are defined and allocated. The implementation of the organisation must ensure segregation of conflicting duties and areas.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **6.1.1 Information security roles and responsibilities**<br>*All information security responsibilities should be defined and allocated.*<br>Information security responsibilities are defined and allocated. | By inspection, we have observed that the organisational areas of responsibility have been defined and allocated to relevant personnel. | No exceptions noted. |
| **6.1.2 Segregation of duties**<br>*Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.*<br>Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets. | By inspection of random samples, we have investigated that the critical operating functions at Visma Acubiz A/S have been appropriately segregated and that primary and secondary operating data have been segregated. | No exceptions noted. |
| **6.1.5 Information security in project management**<br>*Information security should be addressed in project management, regardless of the type of the project.*<br>Information security shall be addressed in project management, regardless of the type of the project. | By inspection, we have observed that a policy for information security in project management is in place.<br>From a sample of changes to systems and applications, we observed that a risk analysis has been addressed. | No exceptions noted. |

**7.1 Prior to employment**

**Control objective:** Employees and contractors are made aware of their roles and responsibilities regarding information security. In addition, employees are screened.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **7.1.1 Screening**<br>*Background verification checks on all candidates for employment should be carried out in accordance with relevant laws, regulations and ethics and should be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.*<br>Background verification checks on candidates for employment are carried out in accordance with relevant laws, regulations and ethics in proportion to the business requirements, the classification of the information to be accessed, and the perceived risks. | We have observed that an HR process is in place to ensure that criminal records are presented before employment starts for both employees and external consultants.<br>From a sample of new hires, we observed that criminal records have been acquired before employment starts. | No exceptions noted. |
| **7.1.2 Terms and conditions of employment**<br>*The contractual agreements with employees and contractors should state their and the organisation's responsibilities for information security.*<br>The contractual agreements with employees and contractors state their and the organisation's responsibilities for information security. | Using random samples, we observed that confidentiality agreements are used in accordance with the guidelines, including:<br>• that employees sign confidentiality agreements at the time of employment<br>• that external consultants sign confidentiality agreements prior to starting work. | No exceptions noted. |

**7.2 During employment**

**Control objective:** Management requires employees and contractors to be aware of their information security responsibilities. Awareness and training in information security responsibilities must be performed.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **7.2.2 Information security awareness, education and training**<br>*All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.*<br>Employees of the organisation and, where relevant, contractors receive appropriate awareness education and training according to agreed-upon levels and regular updates in organisational policies and procedures, as relevant for their job function. | We have observed that Visma Acubiz A/S runs introductory courses for new employees during which information security requirements are explained. We have observed that employees are enrolled in mandatory training programmes at regular intervals for the purpose of ensuring compliance with the security requirements of the organisation. | No exceptions noted. |

**8.1 Responsibility for assets**

**Control objective:** Information assets that are a part of the supply chain must be identified, and the owner and the acceptable use of such assets must be defined and implemented.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **8.1.1 Inventory of assets**<br>*Assets associated with information and information-processing facilities should be identified, and an inventory of these assets should be drawn up and maintained.*<br>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 observed that adequate controls are in place to ensure documentation and maintenance of the inventory of assets. | No exceptions noted. |
| **8.1.3 Acceptable use of assets**<br>*Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.*<br>Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented. | We have observed that all types of identified assets are listed in the acceptable use policy.<br>We have observed that updates to the acceptable use policy are communicated to employees.<br>We have observed that a process is in place to maintain an approved whitelist of allowed services and applications. | No exceptions noted. |

**8.2 Information classification**

**Control objective:** Classification of information must be implemented to ensure the proper protection according to legal requirements and according to the value, sensitivity, and criticality to the organisation. Assets must be handled according to their classification.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **8.2.1 Classification of information**<br>*Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.*<br>Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification. | We have observed that a classification scheme is maintained and has been made available for employees.<br>We have observed that the classification scheme has been reviewed and approved. | No exceptions noted. |

**9.1 Business requirements of access control**

**Control objective:** Requirements to the access control of systems, networks and network services must be identified, reviewed and implemented.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **9.1.1 Access control policy**<br>*An access control policy should be established, documented and reviewed based on business and information security requirements.*<br>An access control policy is established, documented and reviewed based on business and information security requirements. | We have observed that guidelines on access controls have been established, reviewed and approved. | No exceptions noted. |
| **9.1.2 Access to networks and network services**<br>*Users should only be provided with access to the network and network services that they have been specifically authorised to use.*<br>Users are only provided with access to the network and network services that they are specifically authorised to use. | By inspection of random samples, we have observed that access to network and network services is granted based on employees' job function and manager approvals. | No exceptions noted. |

**9.2 User access management**

**Control objective:** User access administration procedures must be established to prevent unauthorised access to systems and services.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **9.2.1 User registration and de-registration**<br>*A formal user registration and de-registration process should be implemented to enable assignment of access rights.*<br>A formal user registration and de-registration process is implemented to enable assignment of access rights. | We have observed that procedures for user administration have been established. By inspection of random samples, we have furthermore observed that the user registration and de-registration process has been implemented. | No exceptions noted. |
| **9.2.3 Management of privileged access rights**<br>*The allocation and use of privileged access rights should be restricted and controlled.*<br>The allocation and use of privileged access rights are restricted and controlled. | By inspection, we have observed that Visma Acubiz A/S has established formalised procedures for user administration and rights management and that these also apply to users with privileged rights.<br>We have observed that authorisation granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior. | No exceptions noted. |
| **9.2.5 Review of user access rights**<br>*Asset owners should review users' access rights at regular intervals.*<br>Asset owners review users' access rights at regular intervals. | By inspection, we have observed that user access rights are reassessed once every six months. | No exceptions noted. |
| **9.2.6 Removal or adjustment of access rights**<br>*The access rights of all employees and external users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.*<br>The access rights of employees and external users to information and information processing facilities are removed upon termination of their employment, contract or agreement, or adjusted upon change. | By inspection, we have investigated that regular follow-up is performed on user rights in operating environments and that these rights are granted based on users' job function.<br>By inspection, we have investigated that terminated users are removed in the operating environment in a timely manner after termination. | No exceptions noted. |

**11.1 Secure areas**

**Control objective:** Physical security requirements must be defined and established to prevent unauthorised physical access to the organisation's facilities.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **11.1.1 Physical security perimeter**<br>*Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.*<br>Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities. | By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. | No exceptions noted. |
| **11.1.2 Physical entry controls**<br>*Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.*<br>Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel are allowed access. | By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved.<br>We have observed that Visma Acubiz A/S has implemented appropriated entry controls to protect physical facilities. | No exceptions noted. |
| **11.1.3 Securing offices, rooms and facilities**<br>*Physical security for offices, rooms and facilities should be designed and applied.*<br>Physical security for offices, rooms, and facilities shall be designed and applied. | By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved.<br>We have observed that Visma Acubiz A/S has implemented appropriated entry controls to protect physical facilities. | No exceptions noted. |

**12.1 Operational procedures and responsibilities**

**Control objective:** Changes that affect information security are controlled. Development, test and operational environments are separated.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **12.1.2 Change management**<br>*Changes to the organisation, business processes, information processing facilities and systems that affect information security should be controlled.*<br>Changes to the organisation, business processes, information processing facilities and systems that affect information security shall be controlled. | We have observed that a formal policy for changes to the organisation, business processes, information processing facilities and systems is maintained.<br>We have observed that a formal policy for changes to the organisation, business processes, information processing facilities and systems has been reviewed and approved.<br>We have inspected a samples of changes to systems and applications and observed that the formal development procedure has been implemented. | No exceptions noted. |
| **12.1.4 Separation of development, testing and operational environments**<br>*Development, testing and operational environments should be separated to reduce the risks of unauthorised access or changes to the operational environment.*<br>Development, testing and operational environments shall be separated to reduce the risks of unauthorised access or changes to the operational environment. | We have observed that in accordance with procedures, Visma Acubiz A/S has established separate environments for development, testing and operation and appropriate segregation of duties in connection with the operation of new functionality. | No exceptions noted. |

**12.2 Protection from malware**

**Control objective:** Regulations on software installation are defined and communicated. A software acquisition process is established and implemented.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **12.2.1 Controls against malware**<br>*Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.*<br>Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. | By inspection of random samples, we have observed that employees' computers at Visma Acubiz A/S are protected by anti-virus software – and that this software is up to date. | No exceptions noted. |

**12.3 Backup**

**Control objective:** Backup of information and software is taken regularly and restore of backups is tested.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **12.3.1 Information backup**<br>*Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.*<br>Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy. | We have observed that requirements regarding backup have been established in the contract with sub-contractors that provide services where backup is relevant.<br>We have observed that a full restore test of IT environments has been performed. | No exceptions noted. |

**12.4 Logging and monitoring**

**Control objective:** Requirements on logs for tracing information security events and suspicious user activity must be defined and implemented. Logs must be reviewed, and requirements on the protection of logs must be defined.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **12.4.1 Event logging**<br>*Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.*<br>Event logs recording user activities, exceptions, faults and information security events are produced, kept and reviewed according to requirements stipulated in the established log documentation overview. | We have observed that event logging of user activities, exceptions, faults and information security events has been configured.<br>We have observed that a log documentation overview stipulates when log reviews must be performed. | No exceptions noted. |
| **12.4.2 Protection of log information**<br>*Logging facilities and log information should be protected against tampering and unauthorised access.*<br>Logging facilities and log information are protected against tampering and unauthorised access. | By inspection, we have observed that Visma Acubiz A/S has established logging facilities that are accessible only to employees whose job function justifies such access.<br>We have observed that log information cannot be edited or deleted. Also, Visma Acubiz A/S performs backup of the log information several times a day, and access is restricted to a few people. | No exceptions noted. |

**12.6 Technical vulnerability management**

**Control objective:** Applications and systems must be protected against vulnerabilities by regular vulnerability scans and follow-up. User software installation governance must be implemented.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **12.6.1 Management of technical vulnerabilities**<br>*Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.*<br>Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk. | We have observed that an annual cycle for the activities regarding management of technical vulnerabilities is maintained.<br>We have observed that penetration tests are performed based on the annual cycle.<br>We have inspected that results from penetration tests are reviewed and follow-up actions are performed. | No exceptions noted. |
| **12.6.2 Restrictions on software installation**<br>*Rules governing the installation of software by users should be established and implemented.*<br>Rules governing the installation of software by users shall be established and implemented. | We have observed that installation of software is restricted to users with a work-related need.<br>We have observed that a whitelist is maintained of all allowed applications and services. | No exceptions noted. |

**13.1 Network security management**

**Control objective:** Networks must be managed and segregated to ensure protection against unauthorised access.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **13.1.1 Network security management**<br>*Networks should be managed and controlled to protect information in systems and applications.*<br>Networks shall be managed and controlled to protect information in systems and applications. | We have observed that the management of networks has been outsourced to a supplier.<br>We have observed that Visma Acubiz A/S follows up on delivered services from suppliers. | No exceptions noted. |

**14.2 Security in development and support processes**

**Control objective:** Requirements on information security within the development lifecycle must be defined and implemented. Changes must be tested and approved in a secure development environment prior to implementation and verified after implementation.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **14.2.1 Secure development policy**<br>*Rules for the development of software and systems should be established and applied to developments within the organisation.*<br>Rules for the development of software and systems are established and applied to developments within the organisation. | We have observed that a formal policy for secure development of changes to systems and applications is maintained.<br>We have observed that the formal policy for secure development has been reviewed and approved. | No exceptions noted. |
| **14.2.2 System change control procedures**<br>*Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.*<br>Changes to systems within the development lifecycle are controlled by the use of formal change control procedures. | We have observed that a formal policy for secure development of changes to systems and applications has been implemented.<br>From a sample of changes to systems and applications, we observed that the formal development procedure has been implemented. | No exceptions noted. |
| **14.2.3 Technical review of applications after operating platform changes**<br>*When operating platforms are changed, business-critical applications should be reviewed and tested to ensure there is no adverse impact on organisational operations or security.*<br>When operating platforms are changed, business-critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security. | We have observed that a formal policy for secure development of changes to systems and applications has been implemented.<br>From a sample of changes to systems and applications, we observed that technical reviews are performed. | No exceptions noted. |

**14.2 Security in development and support processes**

**Control objective:** Requirements on information security within the development lifecycle must be defined and implemented. Changes must be tested and approved in a secure development environment prior to implementation and verified after implementation.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **14.2.4 Restrictions on changes to software packages**<br>*Modifications to software packages should be discouraged and limited to necessary changes, and all changes should be strictly controlled.*<br>Modifications to software packages are discouraged and limited to necessary changes, and changes shall be strictly controlled. | We have observed that a formal policy for secure development of changes to systems and applications has been implemented.<br>From a sample of changes to systems and applications, we observed that changes are authorised. | No exceptions noted. |
| **14.2.5 Secure system engineering principles**<br>*Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.*<br>Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts. | We have observed that secure principles and requirements have been established, documented, maintained and applied to the change management process.<br>From a sample of changes to systems and applications, we observed that an assessment of security and privacy is performed. | No exceptions noted. |
| **14.2.6 Secure development environment**<br>*Organisations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.*<br>The organisation has established and appropriately protected secure development environments for system development and integration efforts that cover the entire system development lifecycle. | We have observed that a formal policy for secure development of changes to systems and applications has been implemented, including segregation of duties related to development, testing and deployment.<br>From a sample of changes to systems and applications, we observed that segregation of duties is enforced in the secure development lifecycle. | No exceptions noted. |
| **14.2.8 System security testing**<br>*Testing of security functionality should be carried out during development.*<br>Testing of security functionality is carried out during development. | We have observed that a formal policy for secure development of changes to systems and applications has been implemented, including testing of security functionality.<br>From a sample of changes to systems and applications, we observed that testing has been performed. | No exceptions noted. |

**14.2 Security in development and support processes**

**Control objective:** Requirements on information security within the development lifecycle must be defined and implemented. Changes must be tested and approved in a secure development environment prior to implementation and verified after implementation.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **14.2.9 System acceptance testing**<br>*Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.*<br>Acceptance testing programs and related criteria are established for new information systems, upgrades, and new versions. | We have observed that a formal policy for secure development of changes to systems and applications has been implemented, including user acceptance and system acceptance testing.<br>From a sample of changes to systems and applications, we observed that testing has been performed. | No exceptions noted. |

**15.2 Supplier service delivery management**

**Control objective:** Supplier service deliveries must be monitored, reviewed and audited on regular basis.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **15.2.1 Monitoring and review of supplier services**<br>*Organisations should regularly monitor, review and audit supplier service delivery.*<br>The organisation shall regularly monitor, review and audit supplier service delivery. | We have observed that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements.<br>From a sample of signed contracts, we observed that information security requirements have been contractually agreed.<br>From a sample of months, we observed that Visma Acubiz A/S audits key suppliers on a periodic basis, based on agreed information security requirements.<br>We have observed that third-party declarations have been received and processed by Visma Acubiz A/S for key suppliers. | No exceptions noted. |

**16.1 Management of information security incidents and improvements**

**Control objective:** A process for managing information security events must be established and implemented to ensure timely assessment, classification, handling and response.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **16.1.1 Responsibilities and procedures**<br>*Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.*<br>Management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents. | We have observed that a formal and documented incident management process has been reviewed and approved.<br>We have observed that a formal and documented incident management process has been implemented.<br>We have observed that the incident management process has been communicated to employees.<br>We have observed that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system. | No exceptions noted. |
| **16.1.2 Reporting and handling information security events and security breach**<br>*Information security events should be reported through appropriate management channels as quickly as possible.*<br>*Employees and contractors using the organisation's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services.*<br>Information security events should be reported through appropriate management channels as quickly as possible.<br>Employees and contractors using the organisation's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. | We have observed that a formal and documented incident management process related to information security events and breaches has been implemented.<br>We have observed that the incident management processes has been communicated to employees.<br>We have observed that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system and reported through the Information Security Board. | No exceptions noted. |

**16.1 Management of information security incidents and improvements**

**Control objective:** A process for managing information security events must be established and implemented to ensure timely assessment, classification, handling and response.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **16.1.4 Assessment of and decision on information security events**<br>*Information security events should be assessed, and it should be decided if they are to be classified as information security incidents.*<br>Information security events are assessed, and it is decided if they are to be classified as information security incidents. | We have observed that a formal process for assessment and analysis of information security incidents is maintained.<br>From a sample of two months, we observed that the Information Security Board reviews and analyses incidents that are classified as information security incidents. | No exceptions noted. |

**17.1 Information security continuity**

**Control objective:** Requirements on information security continuity must be defined and implemented. Plans for business continuity must be verified and evaluated at regular intervals.

| Visma's control activity | Control tests performed by PwC | Results of tests |
|---|---|---|
| **17.1.1 Planning information security continuity**<br>*The organisation should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.*<br>The organisation has determined its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster. | We have observed that a formal and documented business continuity plan is maintained, reviewed and approved annually.<br>We have observed that a business impact assessment has been performed to establish the requirements of a business continuity plan.<br>We have observed that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel. | No exceptions noted. |

*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."*

**Henrik Malling Madsen**
**Kunde**
*Serienummer: 6d122022-f082-44a3-a6b9-b10357b25efc*
*IP: 77.241.xxx.xxx*
*2024-03-22 12:36:33 UTC*

**Jesper Parsberg Madsen**
**PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231**
**Statsautoriseret revisor**
*Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e*
*IP: 83.136.xxx.xxx*
*2024-03-22 12:42:05 UTC*