Visma Acubiz A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2025 to 31 December 2025 in relation to Visma Acubiz A/S's Acubiz Solution standard operating platform to customers

February 2026

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

Contents

1. Management's assertion 3
2. Independent service auditor's assurance report on the description, design and operating effectiveness of controls 5
3. Description of IT general controls relating to the Acubiz Solution standard operating platform 8
4. Control objectives, control activity, tests and test results 20

Penneo dokumentnøgle: L7Y0D-GRD2E-FV111-8HA0G-LOEL1-YFORV

1. Management's assertion

The accompanying description has been prepared by Visma Acubiz A/S (Visma Acubiz) for customers who have used the 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 the customers themselves, when assessing the risks of material misstatements in their financial statements.

Visma IT is a service organisation that provides infrastructure operation (IaaS) to Visma Acubiz. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Visma Acubiz and excludes the control objectives and related controls of Visma IT. Our evaluation did not extend to controls of Visma IT.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of our controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Visma Acubiz confirms that:

a) The accompanying description in section 3 fairly presents the Acubiz Solution standard operating platform that has processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to the Acubiz Solution standard operating platform 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 the Acubiz Solution standard operating platform, 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 IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to the Acubiz Solution standard operating platform during the period from 1 January 2025 to 31 December 2025

   (iii) Does not omit or distort information relevant to the scope of IT general controls in relation to the Acubiz Solution standard operating platform being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of IT general controls in relation to the Acubiz Solution standard operating platform 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 January 2025 to 31 December 2025. The criteria used in making this statement were that:

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2025 to 31 December 2025.

Copenhagen, February 6 2026
Visma Acubiz A/S

Henrik Malling
CEO

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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 January 2025 to 31 December 2025 in relation to Visma Acubiz' Acubiz Solution standard operating platform to customers

To: Visma Acubiz A/S (Visma Acubiz), its customers and their auditors

Scope

We have been engaged to report on Visma Acubiz' description in section 3 of IT general controls in relation to the Acubiz Solution standard operating platform which has processed customers' transactions throughout the period from 1 January 2025 to 31 December 2025 (the description) and on the suitability of the design and operating effectiveness of controls related to the control objectives stated in the description.

Visma IT is a service organisation that provides infrastructure operation (IaaS) to Visma Acubiz. This report uses the carve-out method, and the description in section 3 includes only the control objectives and related controls of Visma Acubiz and excludes the control objectives and related controls of Visma IT. Our examination did not extend to controls of Visma IT.

The description indicates that certain control objectives specified in the description can be achieved only if complementary customer controls contemplated in the design of Visma Acubiz' controls are suitably designed and operating effectively. This report does not comprise the suitability of the design or operating effectiveness of such complementary user entity controls.

Visma Acubiz' responsibilities

Visma Acubiz is responsible for: preparing the description and accompanying assertion in section 1, including the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; identifying the criteria and designing, implementing and effectively operating controls to achieve the stated control objectives. The control objectives have been specified by Visma Acubiz and are stated in the description.

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 the fairness of Visma Acubiz' description and on the suitability of 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 comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

An assurance engagement to report on the description of a service organisation's system and the suitability of the design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the description and 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 also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by Visma Acubiz and described in section 1.

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

Inherent limitations

Visma Acubiz' 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 Acubiz Solution standard operating platform that the individual customer may consider important in its own particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in the Acubiz Solution standard operating platform. Also, the projection to future periods of any evaluation of the fairness of the presentation of the description, or opinions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria including the control objectives described in Visma Acubiz' assertion in section 1:

a) The description fairly presents how IT general controls in relation to the Acubiz Solution standard operating platform were designed and implemented throughout the period from 1 January 2025 to 31 December 2025

b) The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the specified control objectives would be achieved if the described controls operated effectively throughout the period from 1 January 2025 to 31 December 2025 and user entities applied the complementary customer controls referred to in section 3

c) The controls tested, which together with the complementary customer controls referred to in section 3, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2025 to 31 December 2025.

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

We were engaged to report by Visma Acubiz and, therefore, this report and the description of tests of controls and results thereof in section 4 are intended for the use of Visma Acubiz.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

We permit the disclosure of this report in full only, including the description of tests of controls and results thereof by Visma Acubiz, at its discretion, to customers who have used Visma Acubiz' Acubiz Solution standard operating platform during some or all of the period of 1 January 2025 to 31 December 2025 and their auditors, who have a sufficient understanding to consider it, along with other information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements, without assuming or accepting any responsibility or liability to customers or their auditors on our part.

Our report is not to be used for any other purpose or to be distributed to any other parties.

Aarhus, February 6 2026
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

3. Description of IT general controls relating to the 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 organisation'

The objective of this report is to provide information to auditors of user organisations 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 organisation.

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 organisation is responsible for evaluating this information in relation to the internal control structure in place at their organisation in order to assess the total internal control structure.

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

3.2. Audit scope

This service auditor's 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
- Organisation 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

3.3. Data handling

Visma Acubiz is responsible for daily (Monday-Friday) retrieving of electronic transactions from data providers, for uploading such transactions on servers and for continuously loading the transactions into the customer's setup of the Acubiz Solution if the customer has opted for this.

Visma Acubiz is only responsible for the transport of the transactions and not for the content of individual data files.

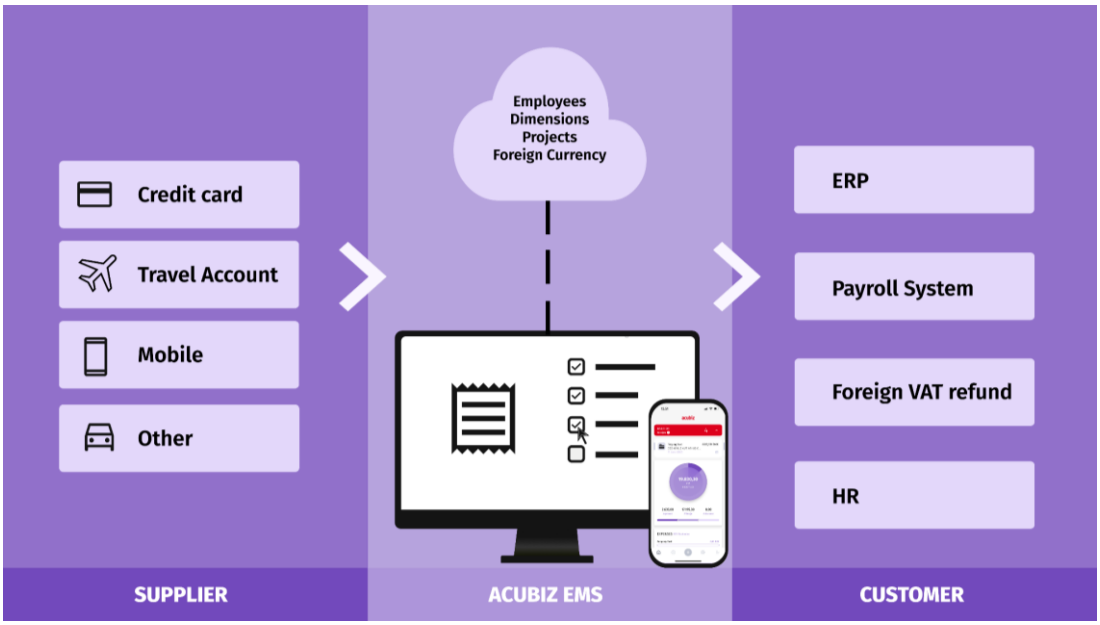
In order to ensure stable operation and to maintain the confidentiality, reliability and accessibility of the Acubiz Solution systems and data, Visma Acubiz has planned processes and controls which protect and cover the customer's business requirements.

3.4. Acubiz Solution

Visma Acubiz was established in 1997 and was based in Birkerød. In December 2021, Visma Acubiz was acquired 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 solution ACUBIZ SOLUTION which is an expense management service.

Acubiz Solution (Standard Version 7) is a web-based expense management service, streamlining the procedures for handling travel 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.

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 an expense report, enter costs and send the expense report for approval and export. Thereafter, the file is ready for import into the company's financial management systems.



Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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:

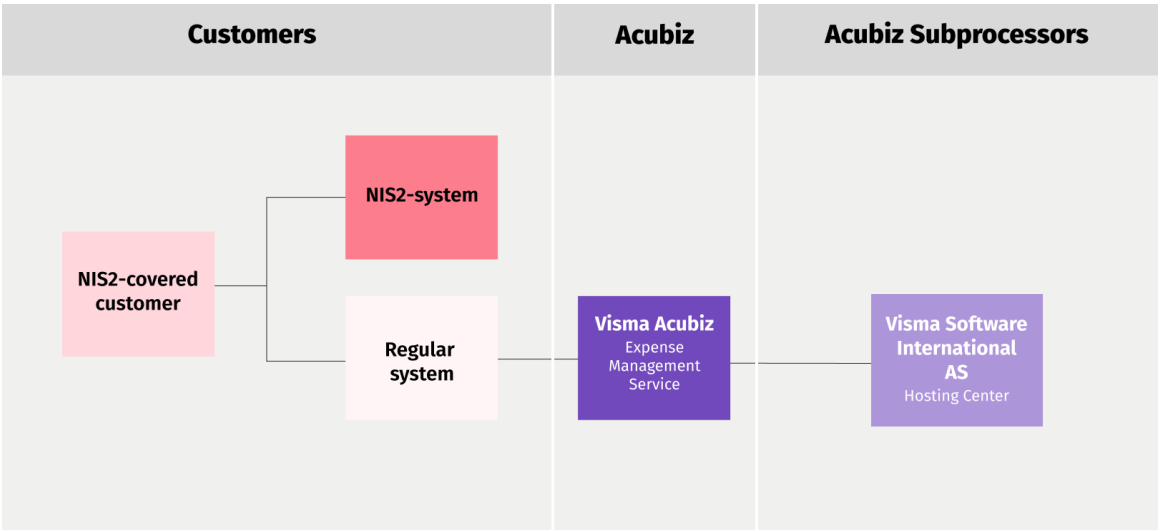
- Pharmaceuticals
- Financial institutions
- Law firms
- Auditors
- Transportation and logistics.

3.4.1. NIS2 and the value chain

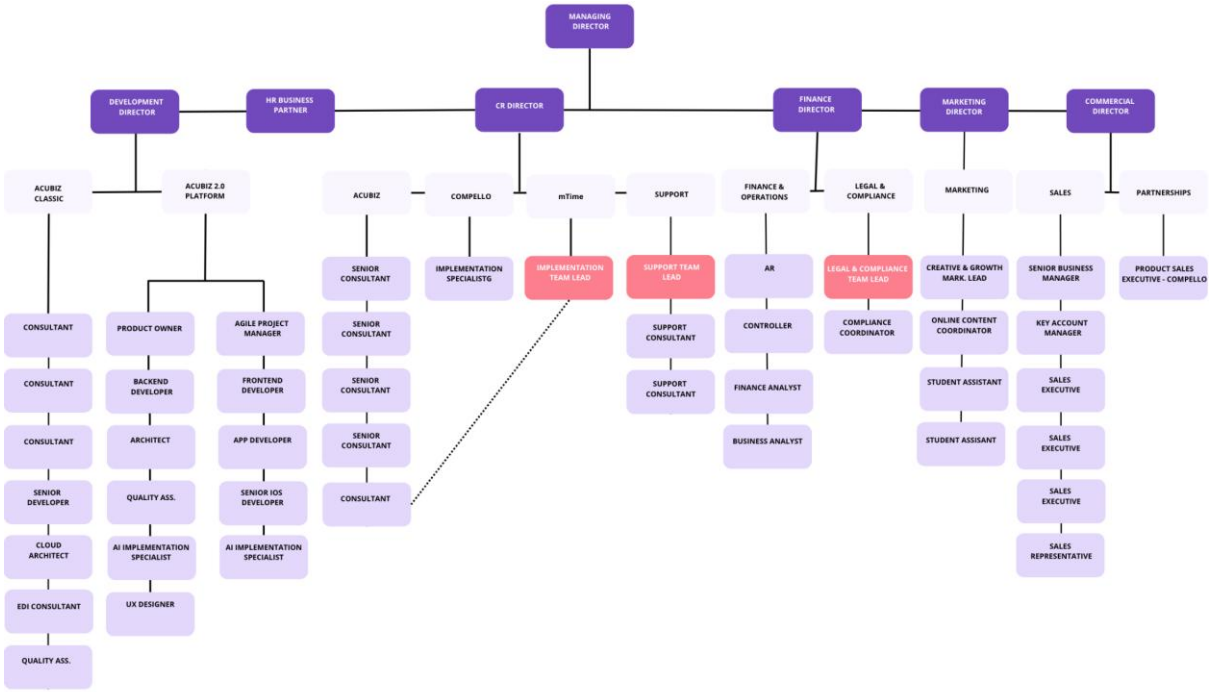
Some of Visma Acubiz' clients are engaged in tasks critical to society and are thus within the scope of the NIS2 directive. However, Visma Acubiz does not provide society-critical services and is therefore not directly subject to NIS2 requirements. In the event that the Acubiz solution is inaccessible, the impact would be limited to the internal processes of Visma Acubiz' customers, without affecting societal functions, including critical societal tasks. The same applies to our subcontractors, who support the Acubiz solution.

Nonetheless, we remain attentive to the new legislation and have proactively implemented controls to reflect these requirements, ensuring that our solution remains compliant.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV



3.5. Organisational structure



Visma Acubiz' legal owners are Visma Denmark Holding. Visma Acubiz' Board consists of three Visma employees, of which one is chairman of the Board and further two persons are board members.

Visma Acubiz' organisation is divided into 10 main areas: "Visma Acubiz Board", "Directors and Management"; "Product and Development", "Operational Excellence and IT-Operation, "Customer Relations", "Marketing", "Sales", "Partnerships", "Finance and Operations" and "HR" which are all grouped under a common management with common administration.

Visma Acubiz Board	Strategy and Business development
Directors and Management	Information Security Board and Product Board
Product and Development	Standard expense management service and customisation, testing and upgrading of customer's solution

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

Operational Excellence and IT-Operation	Hosting, Edi, IT administration, internal and customer-related IT operations
Customer Relations	Implementation and training, Service desk and support functions
Marketing	Digital marketing, Brand and Communication
Sales	Sales and Key account
Partnerships	Sales and third partners (products)
Finance and Operations	Finance, Procurement, Legal & Compliance, Bookkeeping and Payroll
HR	Human Resources

Visma Acubiz has an Information Security Board (ISB) that meets monthly to deal with security and any security incidents. The ISB also assesses whether there are changes in external or internal circumstances that should lead to a reassessment of the preventive or controlling efforts.

Management, Directors, Legal & Compliance Manager and DPM are represented in the ISB.

Management is responsible for the preparation, maintenance and dissemination of security policy, risk assessment, emergency plans, operating routines and documentation of business processes.

The DPM and Legal & Compliance Manager are in charge of the primary contact with accountants and auditors, drive the execution of self-assessments, and prepare and update the contingency plan in collaboration with the ISB.

3.6. Internal control elements at entity level

3.6.1. Control environment

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

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

3.6.2. Control activities

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

3.6.3. 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 organisation may carry out their work satisfactorily with respect to performance as well as time.

Information and communication are an integral part of Visma Acubiz' internal control system. It covers the processes involved in identifying, collecting and exchanging information as well as determining the formats and timelines necessary for effective management and control of the company's operations. Visma Acubiz identifies processes and reports information through various information systems and dialogue with customers, employees and other external stakeholders.

3.6.4. Monitoring

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

Visma Acubiz continuously assesses the overall set of controls to ensure they sufficiently meet the requirements established by our company, our customers and legislation.

3.6.5. Risk assessment

Risk assessment is a critical point in Visma Acubiz' internal control system for handling and continuously assessing risks. The purpose is to identify and classify the risks that may affect the organisation's ability to function and comply with contractual obligations.

Visma Acubiz' Management is aware of the fact that risks must be reported and treated separately in order to counteract and handle them. The challenges faced by Visma Acubiz are therefore assessed and controlled continually based on 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), ISO/IEC 27001 and NIS2 Directive art. 20.

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**

3.6.6. Governance

Visma Acubiz' Management consists of Visma Acubiz' Managing Director, Development Director, Customer Relations Director, Finance & Operations Director, Marketing Director, Commercial Director and HR Business Partner.

Management is generally responsible for preparing policies and ensuring that these are implemented in the organisation, 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 organisation but the general responsibility remains with Management.

Management establishes responsibilities and authorisations for the individual groups or employees in the organisation and determines approval hierarchies as well as rules and procedures for reporting.

3.6.7. Policies and procedures

Executive Management is responsible for policies and practices related to employment (onboarding and offboarding) as well as information, training, evaluation, promotion and compensation of employees. As part of the Visma Group, Visma Acubiz adheres to Visma Group policies, supporting and upholding the organisation's values and attitudes. These policies emphasise the importance of each employee maintaining a high degree of integrity and acting in accordance with the Group's values and current legislation. As part of the employment process, all employees are required to sign a non-disclosure agreement (NDA).

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

3.6.8. Information systems

Visma Acubiz' information systems are grouped into different applications:

- TAW: The Acubiz Way holds descriptions of Visma Acubiz' procedures and processes.
- BITE: This database holds customers' and their database's/databases' master data.
- 360 & HubSpot: These databases hold the registration of the chosen services for each customer.
- STAT: Is Visma Acubiz' 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 their work tasks. Application access is in line with the job function and will therefore be reassessed in the event of changes to the employment.

3.7. Major changes during 2025

In 2025, Visma Acubiz has undertaken significant strategic and operational changes to ensure the continued delivery of a solution built on the newest technology and the highest possible security standards. These changes are focused on reinforcing our internal control environment and enhancing the overall service quality.

Operational and system updates:

- Modernisation of business systems: We have modernised and implemented new back-end systems for business operations, including Hubspot, Younium, Oneflow, Zendesk, ClickUp and Leapsome. This modernisation effort focuses heavily on integrating AI capabilities and optimising data flow and processes across the organisation.

- Enhanced security status: We have advanced from Gold to Platinum status in the Visma Application Security Program (VASP), which is the highest possible achievement in Visma's internal security program. This status confirms our continuous commitment to maintaining high data security standards.

- Implementation of new features: We are currently in the process of implementing major new functionalities, including the more secure MFA login module, Visma Connect, and the new AI-based scanning engine, SmartScan, across our customer base. These improvements aim to enhance both security and efficiency in document handling.

Focus on security and compliance:

- Cybersecurity investment: We are strengthening our efforts in the security domain to effectively counter the increasing threat of cyberattacks. Security remains a top priority, and we continue to invest in the security of the Acubiz solution.

- NIS2 compliance: While the NIS2 Directive does not directly apply to Visma Acubiz and its services, we closely monitor the legislation and remain fully informed about potential indirect obligations. Therefore, our Management has participated in NIS2 e-learning to identify risks and manage their impact on Visma Acubiz' services proactively. This will remain an ongoing task.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

3.8. Description of operations monitoring, including handling of security processes

3.8.1. Information security policy

Visma Acubiz' information security policy.

Based on a risk assessment, a set of information security policies has been established and approved by 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.: 5.1)

3.8.2. Organisation of information security

Internal organisation.

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

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 organisations.

(Control no.: 6.1)

Management is required to complete training on cyber risks, in accordance with NIS2, to enhance their management responsibilities and cybersecurity awareness.

(Control no.: 6.3)

3.8.3. 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 organisation's information security responsibilities.

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

(Control no.: 7.1, 7.2)

3.8.4. Asset management

Visma Acubiz has identified organisational 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 organisation. This includes classification of information in terms of legal requirements, value, criticality and sensitivity to unauthorised 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 unauthorised disclosure, modification, removal or destruction of information stored on media.

(Control no.: 8.1, 8.2)

Penneo dokumentnøgle: L7Y0D-GRD2E-FV111-8HA0G-LOEL1-YFORV

3.8.5. 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 authorised to use.

Visma Acubiz ensures authorised user access to prevent unauthorised 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 organisation's practices in the use of secret authentication information.

(Control no.: 9.1, 9.2)

3.8.6. Physical and environmental security

Visma Acubiz, following Visma Group policy, ensures that unauthorised access to the organisation'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 clean desk, clear screen and removable storage media has been established and implemented.

(Control no.: 11.1)

3.8.7. 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 minimises the risk of exploitation of technical vulnerabilities by an effective patch procedure, penetration testing and continuous vulnerability scanning according to a defined schedule.

(Control no.: 12.1, 12.2, 12.4, 12.6)

3.8.8. Communications security

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

(Control no.: 13.1)

3.8.9. 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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 on 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 formalised ones are:

- Mailbox for wishes from customers (idea.acubiz@visma.com)
- Slack channel for bug reporting #acubiz-product bugs
- Slack channel for product suggestions #acubiz-productsuggestions
- The Product Board.

Priority

Priorities are done at 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 (14.2.2).

Test

All implementations are finalised 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, 14.2.9).

Release

We release to new and pilot customers first and, if successful, mass releases in batches of 50-100 customers are 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 planned functions have been developed, a new version is then created to be ready for 3D 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. Individual sprints containing a new feature are closed/saved as a new version, and this version is made available to one or more customers who 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' internal control has the overall responsibility for ensuring that periodic controls are carried out.

(Control no.: 14.2)

Penneo dokumentnøgle: L7Y0D-GRD2E-FV111-8HA0G-LOEL1-YFORV

3.8.10. Supplier relationships

Visma Acubiz utilises subservice organisations for certain purposes.

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

- Visma Software International AS
  Visma Acubiz has outsourced part of its operation to Visma Software International AS. Visma Acubiz receives independent service auditor's reports covering the operations delivered by the subservice provider.
  The reports are prepared in accordance with ISO 27001, ISAE 3402 and ISAE 3000. Visma Software International AS is 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 reviews the supplier's fulfilment of the information security requirements.

(Control no.: 15.2)

3.8.11. 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.: 16.1)

3.8.12. Information security aspects of business continuity management

A business impact assessment has been performed, and 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. Additionally, tests of our incident response plan have been completed throughout the year to ensure its effectiveness and make necessary updates.

(Control no.: 17.1)

Please refer to section 4 for further description of control objectives and procedures.

3.9. Complementary user entity controls

Visma Acubiz' services are designed on the assumption that certain controls are implemented by user organisations.

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

The list below describes additional controls that should be in operation in customer organisations 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 organisations:

- Visma Acubiz' customers are responsible for validation of their data input in Acubiz Solution.
- Visma Acubiz' customers carry out physical access control on their own premises.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV111-8HA0G-LOEL1-YFORV

- Visma Acubiz' customer users have logical access control (login).
- Visma Acubiz' customers are responsible for their own creation and removal of users. They are also responsible for ensuring that user rights are granted based on a work-related need.
- Visma Acubiz' customers are responsible for testing that the specific customisation is working as required.
- Visma Acubiz' 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 as a comprehensive listing of the control policies and procedures which would provide a basis for the assertions underlying clients' financial statement.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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

4.1. Purpose and scope

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", and additional requirements applicable in Denmark.

Our testing of the design, implementation and operating effectiveness of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2. Test actions

The test actions performed when determining the operating effectiveness of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals.
Inquiries	Inquiry of appropriate personnel. Inquiries included how the controls are performed.
Observation	We observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We repeated the execution of the control to verify whether the control functions as assumed.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

4.3. Overview of 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.

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
6.1.1	**Information security roles and responsibilities** *All information security responsibilities should be defined and allocated.* Information security responsibilities are defined and allocated.	We inspected that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No exceptions noted.
6.1.2	**Segregation of duties** *Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.* Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.	We inspected 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** *Information security should be addressed in project management, regardless of the type of the project.* Information security is addressed in project management, regardless of the type of the project.	We inspected that a policy for information security in project management is in place. From a sample of changes to systems and applications, we observed that a action plan has been addressed.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
6.3	**Information security awareness, education and training** *Management is required to complete training on cyber risks, in accordance with NIS2, to enhance their management responsibilities and cybersecurity awareness.* Management is required to complete training on cyber risks, in accordance with NIS2, to enhance their management responsibilities and cybersecurity awareness.	We observed that Management is continuously being trained in awareness and knowledge of new upcoming legislation relevant to the services provided.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

7.1: Prior to employment

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
7.1.1	**Screening** *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.* 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 observed that an HR process is in place to ensure that criminal records are presented before employment starts for both employees and external consultants. 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** *The contractual agreements with employees and contractors should state their and the organisation's responsibilities for information security.* 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: • that employees sign confidentiality agreements at the time of employment • that external consultants sign confidentiality agreements prior to starting work.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
7.2.2	**Information security awareness, education and training** *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.* 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 observed that Visma Acubiz A/S runs introductory courses for new employees during which information security requirements are explained. We 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
8.1.1	**Inventory of assets** *Assets associated with information and information-processing facilities should be identified, and an inventory of these assets should be drawn up and maintained.* Assets associated with information and information processing facilities are identified, and an inventory of these assets is drawn up and maintained.	We 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** *Rules for the acceptable use of information and of assets associated with information and information processing facilities should be identified, documented and implemented.* Rules for the acceptable use of information and of assets associated with information and information processing facilities are identified, documented and implemented.	We observed that all types of identified assets are listed in the acceptable use policy. We observed that updates to the acceptable use policy are communicated to employees. We observed that a process is in place to maintain an approved whitelist of allowed services and applications.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
9.1.1	**Access control policy** *An access control policy should be established, documented and reviewed based on business and information security requirements.* An access control policy is established, documented and reviewed based on business and information security requirements.	We observed that guidelines on access controls have been established, reviewed and approved.	No exceptions noted.
9.1.2	**Access to networks and network services** *Users should only be provided with access to the network and network services that they have been specifically authorised to use.* Users are only provided with access to the network and network services that they are specifically authorised to use.	We inspected that access to network and network services is granted based on employees' job function and manager approvals.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

9.2: User access management

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

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
9.2.1	**User registration and de-registration** *A formal user registration and de-registration process should be implemented to enable assignment of access rights.* A formal user registration and de-registration process is implemented to enable assignment of access rights.	We observed that procedures for user administration have been established. We inspected that the user registration and de-registration process has been implemented.	No exceptions noted.
9.2.3	**Management of privileged access rights** *The allocation and use of privileged access rights should be restricted and controlled.* The allocation and use of privileged access rights are restricted and controlled.	We inspected 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. We 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** *Asset owners should review users' access rights at regular intervals.* Asset owners review users' access rights at regular intervals.	We inspected that user access rights are reassessed once every six months.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

9.2: User access management

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

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
9.2.6	**Removal or adjustment of access rights** 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. 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.	We inspected that regular follow-up is performed on user rights in operating environments and that these rights are granted based on users' job function. We inspected that terminated users are removed in the operating environment in a timely manner after termination.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

11.1: Secure areas

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

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

12.1: Operational procedures and responsibilities

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

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
12.1.2	**Change management** *Changes to the organisation, business processes, information processing facilities and systems that affect information security should be controlled.* Changes to the organisation, business processes, information processing facilities and systems that affect information security are controlled.	We observed that a formal policy for changes to the organisation, business processes, information processing facilities and systems is maintained. We observed that a formal policy for changes to the organisation, business processes, information processing facilities and systems has been reviewed and approved. We inspected that follow-up is being done regarding Visma IT and audit reports.	No exceptions noted.
12.1.4	**Separation of development, testing and operational environments** *Development, testing and operational environments should be separated to reduce the risks of unauthorised access or changes to the operational environment.* Development, testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.	We 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

12.2: Protection from malware

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

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
12.2.1	**Controls against malware** *Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.* Detection, prevention and recovery controls to protect against malware are implemented, combined with appropriate user awareness.	We inspected 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.

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
12.4.1	**Event logging** *Event logs recording user activities, exceptions, faults and information security events should be produced, kept and regularly reviewed.* 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 observed that event logging of user activities, exceptions, faults and information security events has been configured. We observed that a log documentation overview stipulates when log reviews must be performed.	No exceptions noted.
12.4.2	**Protection of log information** *Logging facilities and log information should be protected against tampering and unauthorised access.* Logging facilities and log information are protected against tampering and unauthorised access.	We inspected that Visma Acubiz A/S has established logging facilities that are accessible only to employees whose job function justifies such access. We 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

13.1: Network security management

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

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

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
14.2.1	**Secure development policy** *Rules for the development of software and systems should be established and applied to developments within the organisation.* Rules for the development of software and systems are established and applied to developments within the organisation.	We observed that a formal policy for secure development of changes to systems and applications is maintained. We observed that the formal policy for secure development has been reviewed and approved.	No exceptions noted.
14.2.2	**System change control procedures** *Changes to systems within the development lifecycle should be controlled by the use of formal change control procedures.* Changes to systems within the development lifecycle are controlled by the use of formal change control procedures.	We observed that a formal policy for secure development of changes to systems and applications has been implemented. 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** *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.* 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 observed that a formal policy for secure development of changes to systems and applications has been implemented. From a sample of changes to systems and applications, we observed that technical reviews are performed.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
14.2.4	**Restrictions on changes to software packages** *Modifications to software packages should be discouraged and limited to necessary changes, and all changes should be strictly controlled.* Modifications to software packages are discouraged and limited to necessary changes, and changes are strictly controlled.	We observed that a formal policy for secure development of changes to systems and applications has been implemented. 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** *Principles for engineering secure systems should be established, documented, maintained and applied to any information system implementation efforts.* Principles for engineering secure systems are established, documented, maintained and applied to any information system implementation efforts.	We observed that secure principles and requirements have been established, documented, maintained and applied to the change management process. 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** *Organisations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.* The organisation has established and appropriately protected secure development environments for system development and integration efforts that cover the entire system development lifecycle.	We 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. 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
14.2.8	**System security testing** *Testing of security functionality should be carried out during development.* Testing of security functionality is carried out during development.	We observed that a formal policy for secure development of changes to systems and applications has been implemented, including testing of security functionality. From a sample of changes to systems and applications, we observed that testing has been performed.	No exceptions noted.
14.2.9	**System acceptance testing** *Acceptance testing programs and related criteria should be established for new information systems, upgrades and new versions.* Acceptance testing programs and related criteria are established for new information systems, upgrades and new versions.	We observed that a formal policy for secure development of changes to systems and applications has been implemented, including user acceptance and system acceptance testing. From a sample of changes to systems and applications, we observed that testing has been performed.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

15.2: Supplier service delivery management

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

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
15.2.1	**Monitoring and review of supplier services** *Organisations should regularly monitor, review and audit supplier service delivery.* The organisation regularly monitors, reviews and audits supplier service delivery.	We 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. From a sample of signed contracts, we observed that information security requirements have been contractually agreed. We observed that third-party assurance reports have been received and processed by Visma Acubiz A/S for key suppliers.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
16.1.1	**Responsibilities and procedures** *Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.* Management responsibilities and procedures are established to ensure a quick, effective and orderly response to information security incidents.	We observed that a formal and documented incident management process has been reviewed and approved. We observed that a formal and documented incident management process has been implemented. We observed that the incident management process has been communicated to employees. We 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 breaches** *Information security events should be reported through appropriate management channels as quickly as possible.* *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.* Information security events are reported through appropriate management channels as quickly as possible. Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We observed that a formal and documented incident management process related to information security events and breaches has been implemented. We observed that the incident management process has been communicated to employees. We 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
16.1.4	**Assessment of and decision on information security events** *Information security events should be assessed, and it should be decided if they are to be classified as information security incidents.* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We observed that a formal process for assessment and analysis of information security incidents is maintained. 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.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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.

No.	Visma Acubiz' control activity	Tests performed by PwC	Result of PwC's tests
17.1.1	**Planning information security continuity** *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.* 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 observed that a formal and documented business continuity plan is maintained, reviewed and approved annually. We observed that a business impact assessment has been performed to establish the requirements of a business continuity plan. We observed that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No exceptions noted.
17.1.2	**Implementing information security continuity** *The organisation should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.* 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 are, together with the continuity management, verified on a regular basis. Additionally, tests of our incident response plan have been completed throughout the year to ensure its effectiveness and make necessary updates.	We observed that a formal and documented business continuity plan is maintained, reviewed and approved annually. We observed that a business impact assessment has been performed to establish the requirements of the business continuity plan.	No exceptions noted.

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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

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

Henrik Malling Madsen
Kunde
Serienummer: 6d122022-f082-44a3-a6b9-b10357b25efc
IP: 77.241.xxx.xxx
2026-02-06 14:00:34 UTC

Mit ID

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 87.49.xxx.xxx
2026-02-06 14:14:30 UTC

Mit ID

Penneo dokumentnøgle: L7Y0D-GRD2E-FV11I-8HA0G-LOEL1-YFORV

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

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

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

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