Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
2300 Copenhagen S

Phone: 36102030
www.deloitte.dk

Visma e-conomic A/S

ISAE 3402 type 2 Service Auditor's Report on General IT Controls related to their Design and Operating Effectiveness for the e-conomic solution throughout the period 1 January 2021 – 31 December 2021

Table of Contents

1 Independent Service Auditor's Report

Independent Service Auditor's Assurance Report on the Description of Controls and their Design

To the management of Visma e-conomic A/S, Visma e-conomic A/S' customers and their auditors.

Scope

We have been engaged to report on Visma e-conomic A/S' (henceforth "Visma e-conomic") description in section 3 of its e-conomic system for processing customers' accounting data from 1 January 2021 – 31 December 2021 (the description), and on the design, implementation and operating effectiveness of controls related to the control objectives stated in the description.

Visma e-conomic uses the subservice providers Google Cloud Platform, Amazon Web Services and Microsoft Azure to perform general IT controls around the production environment for storage and hosting of data, network, infrastructure, application and database servers. Visma e-conomic's system description does not include control objectives and associated controls at the subservice organisations. This report is prepared using the carve-out method, and our testing does not include controls that are carried out by the subservice organisations.

Some of the control objectives described in Visma e-conomic's description of its system can only be achieved if the complementary controls at the user organisations are suitably designed and operating effectively together with the controls at Visma e-conomic. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

Visma e-conomic's Responsibilities

Visma e-conomic is responsible for preparing the description and accompanying assertion in section 2, including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; stating the control objectives; and designing implementing controls to achieve the stated control objectives.

Service Auditor's Independence and Quality Control

We have complied with the requirements for independence and other ethical requirements of the IESBA's Code of Ethics for Professional Accountants, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

Deloitte uses ISQC 1 and therefore maintains a comprehensive system for quality management, including documented policies and procedures for compliance with the Code of Ethics for Professional Accountants, professional standards, and applicable requirements according to the law and other regulations.

Service Auditor's Responsibilities

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

We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "*Assurance Reports on Controls at a Service Organisation*," issued by the International Auditing and Assurance Standards Board. That 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.

An assurance engagement to report on the description, the design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design of controls. The procedures selected depend on the service auditor's judgment, including the assessment that the description is not fairly presented, and that controls are not suitably designed and operated effectively. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation and described in section 2, Visma e-conomic's assertion.

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 e-conomic'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 system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 2. In our opinion, in all material respects:

(a) The description of the general IT controls related to the Visma e-conomic's application (e-conomic) fairly presents, in all material respects, the controls as they were designed and implemented throughout the period 1 January 2021 – 31 December 2021; and
(b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period 1 January 2021 – 31 December 2021; 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 1 January 2021 – 31 December 2021.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those 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 e-conomic, and their auditors, who have a sufficient understanding to consider it along with other information, including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 1 February 2022

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR no. 33 96 35 56

Thomas Kühn
Partner, State-Authorised Public Accountant

2 Visma e-conomic A/S' assertion

The accompanying description has been prepared for customers who have used e-conomic 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 obtaining an understanding of customers' information systems relevant to financial reporting. Visma e-conomic confirms that:

a) The accompanying description in section 3 fairly presents e-conomic for processing of customers' accounting data in the period 1 January 2021 – 31 December 2021. The criteria used in making this assertion were that the accompanying description:

i. Presents how the system was designed and implemented, including:
   - The types of services provided, including, as appropriate, classes of accounting data processed.
   - The procedures, within both information technology and manual systems, by which accounting data were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
   - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for customers.
   - How the system dealt with significant events and conditions, other than accounting data.
   - The process used to prepare reports for customers.
   - Relevant control objectives and controls designed to achieve those objectives.
   - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
   - 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 processing and reporting customers' transactions.

ii. Contains relevant information about changes in the general IT controls carried out during the period from 1 January – 31 December 2021.

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed, implemented and operated effectively in the period 1 January 2021 – 31 December 2021. The criteria used in making this assertion were that:

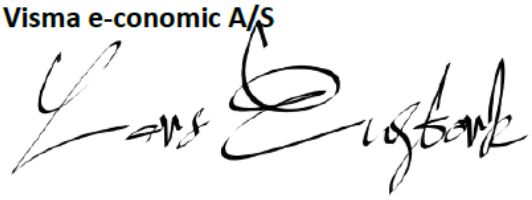
i. The risks that threatened achievement of the control objectives stated in the description were identified; and

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 that;

iii. the controls were applied consistently as designed, including that manual controls were carried out by persons with adequate competencies and authority throughout the entire period from 1 January 2021 – 31 December 2021

Copenhagen, 1 February 2022

Visma e-conomic A/S



Lars Engbork
Managing Director

3 Visma e-conomic A/S' description

3.1 Introduction

Visma e-conomic is a software company selling a cloud-based product called e-conomic, which provides solutions within the areas of ERP, electronic invoicing and accounting to the Danish market.
Visma e-conomic is owned by Visma - a leading provider of core business software for a more efficient and resilient society. Visma simplifies the work of companies and organisations of all sizes, empowering people and helping businesses grow and thrive. Headquartered in Norway, Visma has over 13,600 employees and 1 million customers across the Nordics, Benelux, Central and Eastern Europe and Latin America who share the same passion to **make progress happen**.

By taking advantage of opportunities in a fast-moving market characterised by rapid development in technology, Visma has turned into an international leader in cloud software delivery, and cloud solutions are Visma's top priority.

As a provider of mission critical systems, Visma takes great responsibility when it comes to information security and protecting the privacy of its customers and employees. Being part of the Visma Group, Visma e-conomic is continuously working on improving its security and data protection procedures and practices throughout the organisation.

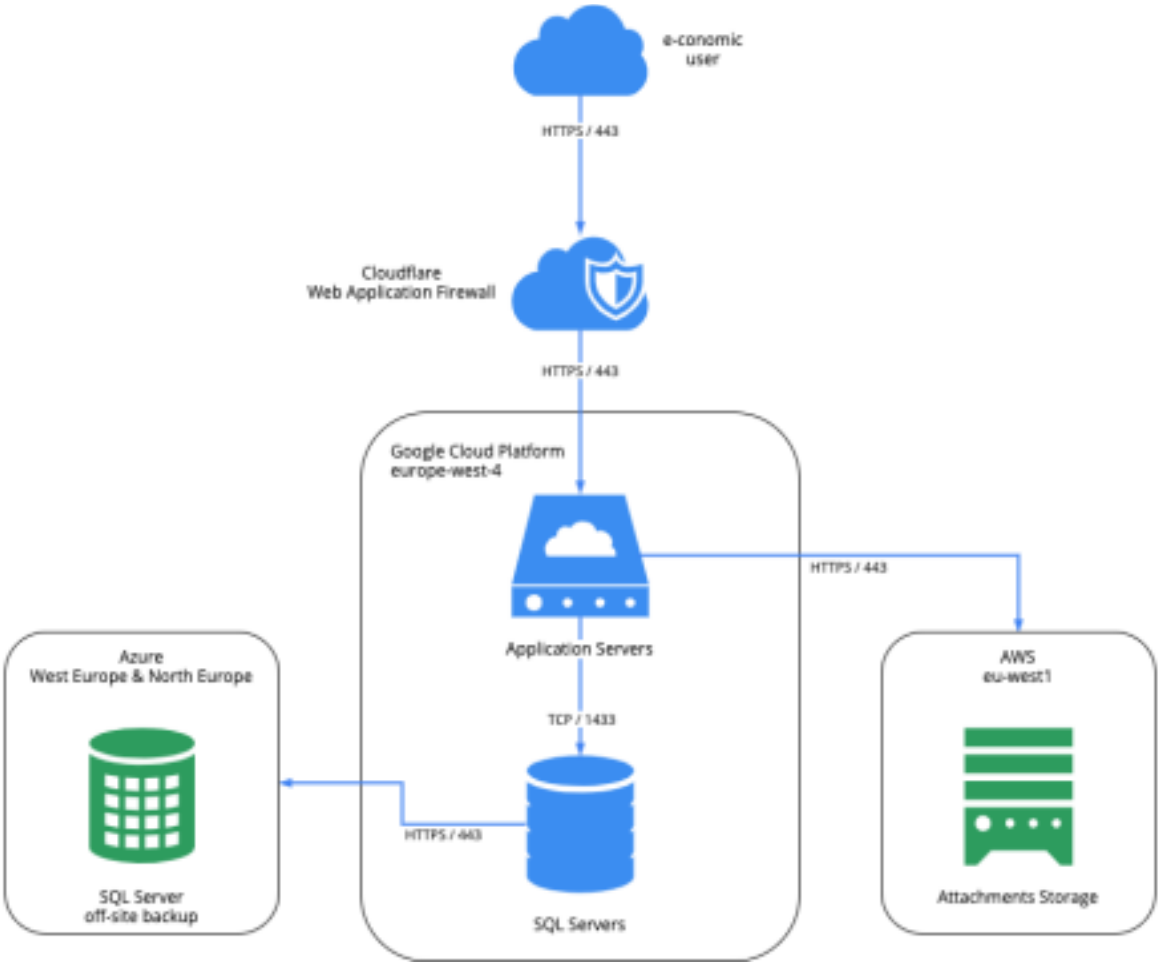
This report is designed to provide information to clients and auditors on the general IT controls applicable to the product, e-conomic. Application controls in e-conomic are not covered in this report.

3.2 Description of Visma e-conomic A/S' services

Visma e-conomic enables small and medium-sized businesses to operate their accounting and bookkeeping practices as expected by Danish law through providing the application, e-conomic. By using e-conomic, customers can handle accounting activities such as invoicing, sales, finance, bookkeeping, VAT accounts and the statements, and reporting.

Via integrations to third-party applications such as time management tools, booking systems and inventory management software, it is possible for businesses to achieve an all-around administration solution. Furthermore, it is possible to upscale the system to have ERP functionalities.

The e-conomic application utilises the Google Cloud Platform for the application and database servers, Amazon S3 for storage of invoice attachments and Microsoft Azure for storage of database backups, as illustrated in the high-level infrastructure diagram below.



3.3 Security governance in Visma Group and Visma e-conomic

The CEO of Visma Group is overall accountable for information security. Responsibility for information security is a line responsibility and distributed throughout all of Visma's business units.

As a part of Visma Group, Visma e-conomic complies with the general policies and procedures set by Visma Group.

3.3.1 Visma Group Security Forum

The Visma Group Security Forum consists of security professionals that represent business units in various parts of Visma Group.

The purpose of this forum is to discuss security-related cases and tasks to identify the issue and propose solutions to mitigate security threats when applicable. The Group Security Forum proposes audits, alterations and additions to Visma Group security policies in addition to guidelines to Visma Group management. The Group Security Forum acts as the supreme council on security-related issues in Visma.

3.3.2 Visma Security Steering Group

The Visma Security Steering Group consists of the Visma CEO, Visma CISO, Visma DPO, division directors and the head of development. The purpose of the group is to:

- Ensure the involvement of all stakeholders impacted by security considerations
- Ensure that security strategy is integrated with business strategy

- Maintain a status on specific actions in the information security programme
- Align on emerging risk, business unit security and compliance issues.

3.3.3 Visma e-conomic Security Forum

The Visma e-conomic Security Forum consists of the Managing Director, Security Project Manager, Data Protection Manager, Director of Engineering and the Director of Core. The Visma e-conomic Security Forum aims to meet monthly.

The purpose of this forum is to make informed decisions when dealing with security and privacy risks on a business unit level. Upon sharing perspectives and understanding issues from different stakeholders, the Visma e-conomic Security Forum maintains a risk register that is used to prioritise the mitigation and elimination of various security and privacy-related risks.

3.3.4 Security Engineers and the Security Guild

Within each product team, Visma e-conomic appoints a Security Engineer to be responsible for all security-related questions and issues. Security Engineers play a significant role in the technical response to product-related security incidents, including investigating the root cause analysis and leading the technical mitigation strategy. Additionally, Security Engineers educate their colleagues in triaging security defaults and help conduct threat modelling in their teams.

The Security Engineers, together with the Security Project Manager and the Director of Engineering, form the Security Guild, which meets bi-monthly to discuss and escalate various security issues within the various teams.

3.3.5 Managers

Managers are responsible for ensuring that policies and procedures are implemented and followed in their respective units/departments/divisions.

3.3.6 All employees

It is the collected practices of all Visma employees that contribute the most to Visma's information security. As an employee, it is important to be aware that risk is often very subjective and that one's own recognition of risk may not coincide with Visma's. It is therefore every employee's responsibility to follow the policies and procedures of Visma.

All employees are responsible for following general security policies and the security provisions of their roles and the procedures they perform. This includes reporting security incidents and violations of Visma's security policies to their nearest manager. All employees are encouraged to suggest improvements to the security policies if the policies are inadequate.

New employees of Visma e-conomic are introduced to the security policies during their onboarding and are subject to ongoing training and awareness throughout the year.

3.4 Control environment

Visma e-conomic has established the following general IT controls to support the delivery of e-conomic (references are to Annex A of ISO 27001:2013):

- Information security policy (A.5)
- Internal organisation (A.6)
- Human resource security (A.7)
- Access control (A.9)
- Operations security (A.12)
- Communications security (A.13)
- System acquisition, development and maintenance (A.14)
- Supplier relationship (A.15)

- Information security incident management (A.16)

3.5 Information security policy (A.5)

3.5.1 Policies for information security

The Visma e-conomic's business is based on information and data, and as such is dependent on the trust of customers, partners, suppliers, shareholders and employees. In order to maintain information security at all levels in the organisation, from support cases and data in the cloud to the confidentiality of business relations, Visma e-conomic abides by the Visma Information Security Policy.

The Information Security Policy addresses the following main areas:
- Risk management
- Organisation and responsibilities for information security
- Acceptable use
- Access controls and access codes
- Software as a Service usage
- Password policies
- Removable storage
- Use of email
- Remote access
- Use of personal devices
- Information classification and handling

The Visma Information Security Policy is managed by the Visma Group Security Forum. Visma Management approves the policies based on recommendations from the Group Security Forum annually. The Visma Information Security Policy is implemented throughout Visma e-conomic in addition to other security policies tailored to fit the practices of Visma e-conomic.

All security policies and guides are available on the intranet for all employees. New employees are made aware of these policies during their onboarding process and employees are subject to ongoing security awareness and training.

3.5.2 Risk Management

Throughout Visma, it is the belief that effective risk management integrated with all organisational processes contributes to the achievement of objectives and improved performance in the working environment, security, legal and regulatory compliance, product quality, project management, operational effectiveness, governance and corporate reputation. To determine risk, Visma e-conomic uses the *risk = impact x likelihood* methodology, with risk, impact and likelihood levels appropriate to Visma e-conomic and its customers. Risk levels take into account information about the asset being protected, the value of the asset, and any vulnerabilities or threats against it.

By identifying all relevant risks that threaten the security and privacy of information, Visma e-conomic is able to maintain an acceptable level of risk through the implementation of technical and organisational controls.

Risk management at Visma e-conomic is implemented on multiple levels. On a high level, the Visma e-conomic Security Forum evaluates risks within the scope of privacy and security and documents them in a risk register. All members of the Forum add to the risk register on a continuous basis and based on impact and likelihood, the risks are prioritised for elimination and mitigation at the Forum.

A risk-based security assessment of the e-conomic application and its components is performed on an annual basis and is reviewed and approved by Visma Group Security and Visma Group Privacy. The purpose is to provide documentation of how Visma e-conomic fulfils certain requirements and recommendations for application security, information security and privacy and data protection and actions that must

be taken in order to improve security and compliance. Actions to be taken are created as tickets, which are prioritised and based on risk to customers and Visma e-conomic.

Visma e-conomic also performs a privacy risk assessment annually in regard to the processing of customers' personal data. The assessment considers the likelihood and impact of the loss of confidentiality, integrity and availability of personal data for the data subjects and Visma. The purpose of this assessment is to evaluate whether the technical and organisational controls in place are sufficient to protect the data processed.

For all third parties that process personal data on behalf of Visma e-conomic and its customers, vendor risk assessments are performed annually. These assessments consider the types and amount of personal data processed by third parties and the controls in place to protect the data, e.g. where data is hosted, level of encryption and deletion procedures. For third parties that process data outside of the EU/EEA, risks are created for the processing of data in third countries. In response, Visma e-conomic performs a Transfer Impact Assessment to evaluate the level of security and privacy in the relevant countries where data is processed.

3.6 Internal organisation (A.6)

3.6.1 Information security roles and responsibilities

As a part of Visma Group, Visma e-conomic complies with the policies and procedures set by Visma Group. Within Visma e-conomic, the management has defined and allocated all information security responsibilities.

The Managing Director has the overall responsibility for the internal security policies in Visma e-conomic. Managers are responsible for the daily information security compliance and contribute towards the achievement of Visma e-conomic's operational information security processes and procedures.

Departments in Visma e-conomic are responsible for the information security and the security of their respective products and services within their own areas. Employees are responsible for maintaining information security in products, services and processes and for reporting security incidents, as necessary.

Additionally, Visma e-conomic has established a Security Forum within the organisation. The high-level security and privacy-related risk register is owned by the Visma e-conomic Security Forum.

3.7 Human resources security (A.7)

3.7.1 Screening

Prior to employment, Visma e-conomic ensures that employees understand their responsibilities and that they are suitable for the roles for which they are considered.

Screening is carried out by the hiring manager in collaboration with HR. Depending on the role and responsibilities the candidate is to take on, there may be more stages for the candidate to pass before reaching the final stage in being offered a contract. These stages may include personality and logic tests, reference calls, and criminal background checks for employees who would gain access to the production SQL server.

All employment contracts include a non-disclosure agreement covering information related to customer data, sales and marketing data, strategy and other confidential business data. Employees are held to confidentiality both during and after employment.

3.7.2 Information Security awareness, education and training

One of Visma e-conomic's main assets is the employees, and Visma e-conomic ensures that the employees receive continuous awareness and training related to security and privacy. This is done by sharing internal knowledge and through offering relevant external courses and certifications for the employees.

All new employees are required to participate in an onboarding session titled 'Introduction to Legal and Compliance', where employees receive an introduction to all internal policies related to data protection as well as a walkthrough of all implemented information security policies.

All policies and procedures are available to employees on the company intranet at all times.

3.8 Access control (A.9)

3.8.1 Access Control Policy

Visma e-conomic ensures that access to information and information processing facilities is limited to those who have a work-related need to do so. The access Control Policy is based on the least privilege principle. Privileged access assignments may be segregated into unit-based groups such as marketing, human resources, customer support or other business units.

Depending on the service system in use, policies may be tailored specifically to provide a default privilege setting for different types of user accounts.

3.8.2 User access provisioning

User access is provisioned with an organisation-wide access management system built on top of Visma's privileged domain accounts. Permissions that touch customer data or introduce production changes in any way are requested as time-based tokens and can only be performed by vetted personnel while producing an audit trail.

3.8.3 Review of user access rights

The team responsible for the production environment within the Product Unit of Visma e-conomic is subject to an additional vetting process to allow self-provisioning of time-based tokens, while all other units must be reviewed and verified at each request by the corresponding service owner. Privileged access is only granted as time-based tokens up to a maximum of 8 hours for specific roles.

Periodic reviews of access rights are performed on a regular basis by the owner of each system.

3.8.4 Removal or adjustment of access rights

Upon termination of employment, Visma e-conomic ensures that employees return all relevant assets, including mobile devices and key cards, and access to data. Regarding access from central systems, Visma Group handles changes to employee roles and terminations upon notification from Visma e-conomic. For any systems not controlled centrally, Visma e-conomic uses an offboarding checklist.

3.8.5 Secure logon procedures

Password requirements for all systems and accounts are described in the Visma Information Security Policy. Employee passwords must meet the length and complexity requirements, and multi-factor authentication should be used where supported. For all work and privileged accounts, employees are automatically enrolled in 2-factor authentication.

3.8.6 Password management system

Visma's Active Directory enforces an industrial standard for length and complexity of the password.
Additionally, Visma e-conomic uses a password management system to enforce strong master passwords and multi-factor authentication when accessing production secrets. Access to the password management system is always logged.

3.9 Operations security (A.12)

3.9.1 Documented operating procedures

Visma e-conomic ensures the 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 environments.

To provide guidance to employees working with operations, Visma e-conomic has created a number of field guides that contain information about essential areas of daily operations.

Information regarding potential incidents in operations are collected, from various tools, and sent to an alerting system, which alerts relevant people at all hours. After an incident, a post-mortem follow up is held to discuss the event, the root cause and actions to be taken.

3.9.2 Change management

The procedure for change management is supported by the agile platform Jira software. The change management procedure ensures that all the changes are approved through peer review before any changes are deployed to production.

3.9.3 Capacity management

Capacity monitoring is done on metrics of the application database. When it shows signs of congestion, an alert is triggered, informing the responsible operational personnel.

Metrics on capacity issues and availability are available through a metrics dashboard system, and historic and current incidents are available on a status page.

3.9.4 Separation of development, testing and operational environments

Development, testing and operational environments are completely separate from each other.

3.9.5 Information backup

Information saved in databases is protected with everyday backup to the local disk and then copied to the external storage. The backup retention period is 90 days on the external storage.
Transaction log backups are performed frequently for point-in-time recovery. The restore test of the production database is performed on a weekly basis.

3.9.6 Event logging

Error and information logs are extracted from application servers as well as database servers. They are stored with specific retention periods for different types of troubleshooting and future references. Logs contain detailed information, including health of the server, health of databases, events and errors.

3.9.7 Protection of log information

Access to log information is managed by Visma Group's centralised identity management system, allowing only Visma e-conomic employees with work-related need access.

3.9.8 Installation of software on operational systems

Visma e-conomic performs a weekly build of the base application image based on the most recent images available with the cloud provider. The most recent base image is then used for all application deployments after completion. This ensures that the latest security patches and updates are applied to all test and production environments. Latest software patch installation on database servers is done on demand, but at least annually with a service window.

3.9.9 Management of technical vulnerabilities

Visma e-conomic minimises the risk of exploitation of technical vulnerabilities by an effective patch procedure as well as regular vulnerability scans of the codebase as well as of the infrastructure.

3.10 Communications security (A.13)

3.10.1 Network controls

Test, staging and production environments are segmented by separate cloud provider subscriptions and by firewall rules and separated from the rest of the Visma e-conomic network. Changes to network infrastructure are handled as peer reviewed code changes.

3.11 System acquisition, development and maintenance (A.14)

3.11.1 System change control procedures

Visma e-conomic ensures that information systems are designed and implemented according to the system development and security life cycle in order to maintain a structured and well-controlled environment. A system development and maintenance policy has been established and implemented and is supported by an established system development and security life cycle (SDLC) and by the use of an established change management workflow.

Large-scale or business-critical roadmap items are discussed and prioritised in the Product Steering Group.
For certain projects, a Project Mandate is written and continuously updated to document major decisions regarding e.g. scope and priorities.

Further documentation on e.g. business logic and technical implementation details is done in JIRA, as the high-level Epic is broken down into Stories and Tasks during either ad-hoc sessions or the individual teams' continuous planning and grooming sessions.

3.11.2 Technical review of applications after operating platform changes

Procedures have been implemented to ensure that all changes to the operating platform have been reviewed and tested before these changes are implemented in production. Following the implementation of changes in the production environment, the tests are repeated to verify that the changes have been successful.

3.11.3 System security testing

Visma e-conomic's development principles ensure that the e-conomic application maintains high quality through the following steps:

- Analysis, development, code review and test supported by JIRA
- Unit tests
- Coverity - automated code scanning test
- Business Acceptance tests to make use cases for an effective test of standard customer scenarios

Furthermore, a Manual Application Vulnerability Assessment (Attack & Penetration) test is performed, as a minimum, on an annual basis.

3.12 Supplier relationships (A.15)

3.12.1 Monitoring and review of supplier services

A process for supplier procurement has been established to ensure classification of suppliers and, if applicable, to ensure that suppliers meet the security requirements.

Visma e-conomic maintains an agreed level of information security and service delivery in line with supplier agreements by monitoring, reviewing, and auditing suppliers on a regular basis. Audits are carried out annually to ensure that Visma e-conomic's sub-processors live up to all obligations set forth in the agreement and maintain a satisfactory security level based on any assessed risks.

3.13 Information security incident management (A.16)

3.13.1 Responsibilities and procedures

Visma e-conomic ensures a consistent and effective approach to the management of information security and/or privacy incidents, including the communication of these incidents to customers when necessary and relevant.

A process for analysing, mitigating, and responding to information security and/or privacy incidents or weaknesses has been established and implemented. All employees are also required to be alert and to notify of any potential security incidents. This includes responding to alarms from systems and customers, partners, etc. to detect weaknesses and potential incidents.

Following each incident, a meeting is held to discuss what happened and how Visma e-conomic responded, document the root cause, and make note of preventative actions to be taken.

3.13.2 Reporting information security events

All Visma e-conomic employees are responsible for reporting potential incidents to the incident response team as soon as possible. Reported information security and/or privacy events and weaknesses are reviewed and classified on a regular basis.

3.14 Complementary user entity controls

e-conomic is designed on the assumption that certain controls should be implemented and operated effectively by the customer in order to achieve certain control objectives in this report.

The list below describes additional controls that should be in operation in the customer's organisation to complement the controls offered by Visma e-conomic. The list does not represent, and should not be considered, an exhaustive list of the control policies and procedures which would provide a basis for the assertions underlying clients' financial statements.
Customers should consider whether the following complementary controls have been implemented and operated effectively within their own organisations:

- Controls to ensure that the customer organisation has proper control over the use of IDs and passwords used for accessing information in e-conomic
- Controls to ensure that the access rights assignments for e-conomic are provided adequately and in compliance with the user's work-related needs
- Controls to ensure that configuration changes are authorised, tested and approved through change management processes related to configuration changes
- Controls to ensure that the data processed in e-conomic is accurate and up to date
- Controls to ensure that physical access to the customer's premises is restricted to authorised individuals.

4 Controls, control objectives, tests and results hereof

4.1 Introduction

This report is intended to provide Visma e-conomic's customers with information about the controls at Visma e-conomic that may affect the processing of user organisations' account data and also to provide Visma e-conomic's customers with information about the design and implementation of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at user organisations, is intended to assist user auditors in (1) planning the audit of user organisations' financial statements and in (2) assessing control risk for assertions in user organisations' financial statements that may be affected by controls at Visma e-conomic.

Our testing of Visma e-conomic's controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organisations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organisation. If certain complementary controls are not in place at user organisations, Visma e-conomic's controls may not compensate for such weaknesses.

4.2 Test of Controls

The test of controls performed consist of one or more of the following methods:

Method	Description
Inquiry	Interview, i.e., inquiry with selected personnel at Visma e-conomic
Observation	Observation of the execution of control
Inspection	Review and evaluation of policies, procedures, and documentation concerning the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance of control	Repetition of the relevant control to verify that the control functions as intended.

4.3 Test of Operating Effectiveness

Our test of the operating effectiveness of controls includes such tests as we consider necessary to evaluate whether those controls performed, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved throughout the period from 1 January 2021 to 31 December 2021.

Our test of the operating effectiveness of controls was designed to cover a representative number of transactions throughout the period from 1 January 2021 to 31 December 2021 for each of the controls listed in this section, which are designed to achieve the specific control objectives. When selecting specific tests of the operating effectiveness of controls, we considered (a) the nature of the areas tested, (b) the types of available documentation, (c) the nature of audit objectives to be achieved, (d) the assessed control risk level, and (e) the expected efficiency and effectiveness of the tests.

4.4 Control objectives, controls, and test results

4.4.1 Information Security Policy (A.5)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To provide management with direction and support for information security in accordance with business requirements and relevant laws and regulations.			
A.5.1.1 *Policies for information security*	Visma e-conomic has prepared a management-approved IT security policy covering relevant information security-related guidelines. The policy has been published and communicated to relevant employees.	Deloitte inspected the IT security policy to ascertain that this was reassuringly designed and approved by management. Deloitte inspected documentation showing that the IT security policy is communicated to relevant employees.	No exceptions noted.
A.5.1.2 *Risk assessment*	Visma e-conomic has prepared a management-approved risk assessment documenting main risks to the business and service offered. The risk assessment is reviewed annually or upon significant changes.	Deloitte inspected the risk assessment to ascertain that this was reassuringly designed and approved by management.	No exceptions noted.
A.5.1.3 *Review of the policies for information security*	The IT security policy and the corresponding risk assessment is evaluated annually or upon significant changes.	Deloitte inspected the IT security policy and the corresponding risk assessment and assessed that the policy and the risk assessment has been reviewed and approved by management.	No exceptions noted.

4.4.2 Organisation of Information Security (A.6)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation.			
A.6.1.1 *Information security roles and responsibilities*	Visma e-conomic has allocated roles and responsibilities in an organisational chart, and the employees are familiar with their tasks and responsibilities to ensure proper handling of security-related activities.	Deloitte inspected the organisational chart and through inquiries verified that the employees understand their tasks and function.	No exceptions noted.

4.4.3 Human resource security (A.7)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. To ensure that employees and contractors are aware of and fulfil their information security responsibilities.			
A.7.1.1 *Screening*	Visma e-conomic is screening job applicants to ensure suitable candidates for the roles intended. Background verification checks on all candidates for employment are carried out, which involves reference calls. For employees with access to customer systems and data, a criminal record is obtained prior to the recruitment of the candidate. All employment contracts include a non-disclosure agreement covering information related to confidential business data.	Deloitte inquired with key personnel about the process for screening. Deloitte inspected the procedures used and the procedures performed for screening. Deloitte inquired with key personnel about the process for signing non-disclosure agreements. For a sample of users created in the audit period, we have inspected documentation showing that a screening of employees with access to customer systems was conducted prior to employment.	No exceptions noted.
A.7.2.2 *Information security awareness, education and training*	Visma e-conomic conducts training related to information security through onboarding sessions with new employees.	Deloitte inspected the latest training material used for training of new employees. Deloitte inspected documentation in order to ascertain that employees participate in information security awareness training.	No exceptions noted.

4.4.4 Access control (A.9)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To limit access to information and information processing facilities.			
A.9.1.1 *Access control policy*	An access control policy is established, documented and reviewed based on business and information security requirements.	Deloitte inspected that an access control policy is established. Deloitte inspected documentation for a sample of users that access to e-conomic has been granted in accordance with the implemented policy.	No exceptions noted.
Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
A.9.2.2 *User access provisioning*	A formal user access procedure is implemented to ensure that access rights are allocated based on position and department.	Deloitte inspected that a procedure for user provisioning is in place. Deloitte observed that a system is used for user access provisioning. Deloitte inspected documentation for a sample of users that the process for user access provisioning has been implemented and operating in accordance with the procedure.	No exceptions noted.
A.9.2.5 *Review of user access rights*	A formal access procedure is implemented to ensure that time-based token access to the production environment must be reviewed and verified at each request by the corresponding service owner. User access provisions for users with access to customer data or systems are managed by a system, which is based on requesting time-based tokens. Requests are approved by the immediate manager.	Deloitte inspected the procedures for granting time-based token access to Visma e-conomic production environment. Deloitte observed that a system is used for requesting time-based token access. Deloitte inspected documentation for a sample of users that the process for time-based access has been implemented and operating in accordance with the procedure.	No exceptions noted.
A.9.2.6 *Removal or adjustment of access rights*	Visma e-conomic has established a procedure for closing user accounts or disabling users. HR is notified, and they subsequently close the internal directory accounts. Disabling the user in the directory will prevent the user from accessing development-related systems.	Deloitte inspected the procedures for removal or adjustment of access rights. Deloitte inspected documentation for a sample of users that the process for closing down users has been implemented and operating in accordance with the procedure.	No exceptions noted.

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To prevent unauthorised access to systems and applications.			
A.9.4.2 *Secure log-on procedures*	A password policy has been established in Visma e-conomic's information security policy. Passwords are configured as follows. • Password length regular user: 15 characters • Password length admin user: 20 characters • Change on the first login: Yes • Multi-Factor Authentication: Mandatory when supported by the system and mandatory for all new systems. • Change Interval: When a password breach has been detected.	Deloitte inspected the procedures for use of passwords. Deloitte inspected the password settings on Windows AD and the password tool '1password' in order to ascertain whether passwords have been configured in alignment with policies. Deloitte inspected that administrative passwords are handled through the password tool '1password'.	No exceptions noted.
A.9.4.3 *Password management system*	Password management systems are interactive and ensure passwords of good quality.	Deloitte inspected procedures for administrative passwords. On a sample basis, Deloitte inspected that administrative passwords are handled through the tool '1password'. On a sample basis, Deloitte inspected documentation from '1password' in order to ensure that storage of passwords, access and password requirements are in accordance with the procedure.	No exceptions noted.

4.4.5 Operations security (A.12)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure correct and secure operations of information processing facilities.			
A.12.1.1 *Documented operation procedures*	Visma e-conomic has written guidelines and procedures for operations, development and maintenance of systems.	Deloitte inspected and reviewed the procedures that are in place at Visma.	No exceptions noted.
A.12.1.2 *Change management*	Visma e-conomic has defined change management procedures regarding secure development, test and deployment processes.	Deloitte inspected the procedures for change management and that they cover considerations on secure development, test and deployment. Deloitte inspected documentation for a sample of changes that the process for change management has been implemented and operating in accordance with the procedure.	No exceptions noted.
A.12.1.3 *Capacity management*	Visma e-conomic has implemented a process for capacity management, which is supported by various tools to monitor capacity and operational errors. Visma e-conomic has established a status page in e-conomic showing historical and current incidents.	Deloitte inspected the procedure concerning monitoring and adjustment of capacity to ensure availability. On a sample basis, inspected the use of tools for monitoring. Deloitte inspected the e-conomic status page showing incident reporting to customers regarding capacity monitoring. Deloitte inspected documentation for a sample of capacity alarms that the process for monitoring and adjustment of capacity to ensure availability has been implemented and operating in accordance with the procedure.	No exceptions noted.
A.12.1.4 *Separation of development, testing and operational environments*	Visma e-conomic has separated development, test and production environments on different servers.	Deloitte inspected documentation showing separation of development, testing and operating environments.	No exceptions noted.
Control objective: To protect against loss of data.			
A.12.3.1 *Information backup*	Visma e-conomic has established backup procedures for e-conomic.	Deloitte inspected the backup procedures to assess whether backup procedures are adequate.	No exceptions noted.

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
	Restoration of data from backup systems is tested regularly. Backups are stored locally as well as externally at another geographical and secure location.	Deloitte inspected documentation regarding the backup configurations to assess whether these are implemented in accordance with the backup procedures. Deloitte inspected documentation for a sample of restore tests that restore from backup has been performed in accordance with the procedure.	
Control objective: To record events and generate evidence.			
A.12.4.1 *Event logging*	Event logging of user activity, exceptions and errors is enabled and stored with specific retention periods, for the sake of future studies and monitoring of access control.	Deloitte observed the log mechanisms and procedures regarding security logging in general. Deloitte inspected, for a sample of user logs, that user access is logged.	No exceptions noted.
A.12.4.2 *Protection of log information*	Logging facilities are protected from unauthorised access by the security measures established on the servers. Access to log information is limited by the operating system's user control on the machines where data is stored. Access to log information is granted by time-based tokens and is restricted with view access.	Deloitte inquired with key personnel whether procedures are in place for safeguarding logs. On a sample basis, Deloitte has inspected that only employees with a work-related need have access to the logs. Deloitte inspected documentation for a sample that the process for time-based access has been implemented and operating in accordance with the procedure.	No exceptions noted.
Control objective: To ensure the integrity of operational systems.			
A.12.5.1 *Installation of software on operational systems*	Software installations on operating software are updated weekly with most recent updates that are supported by the supplier.	Deloitte inquired with key personnel whether procedures are in place for patch management. Deloitte inspected documentation for a sample of patches that the installation and upgrade are performed in accordance with the procedure.	No exceptions noted.

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To prevent exploitation of technical vulnerabilities.			
A.12.6.1 *Management of technical vulnerabilities*	Information about technical vulnerabilities on e-conomic shall be obtained in a timely fashion, the organisation's exposure to such vulnerabilities is evaluated and appropriate measures are taken to address the associated risks.	Deloitte inspected the procedures for monitoring and handling technical vulnerabilities for e-conomic. Deloitte inspected documentation for a sample of vulnerability scans performed, and evaluated that appropriate measures are taken to deal with associated risks.	No exceptions noted.

4.4.6 Communications security (A.13)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure the protection of information in networks and its supporting information processing facilities.			
A.13.1.1 *Network controls*	Visma e-conomic has secured the network to avoid unauthorised access, through access control and separation of network services. Network firewalls are installed to protect information in e-conomic. Changes to network infrastructure are handled as peer reviewed code changes.	Deloitte inspected the procedure for management and control of the network. On a sample basis, Deloitte inspected implemented network controls to assess whether they are in accordance with implemented procedures. Deloitte inspected documentation of firewall rules implemented in e-conomic. Deloitte inspected documentation showing that a sample of changes to network infrastructure has been reviewed and approved by peer review prior to deployment.	No exceptions noted.
A.13.1.3 *Segregation in networks*	The network is configured into separate networks for production and guest networks. The production network does not allow for access from within the guest network. Wireless network access requires a valid username and password as well as the use of authorised equipment. Visma e-conomic has segregated the network into subnets covering internal-, staging-, sandbox- and production environments.	Deloitte inspected the segregation of networks and verified that access to the wireless network requires a username and a password. Deloitte inspected documentation for the segregation of networks in subnets.	No exceptions noted.

4.4.7 System acquisition, development and maintenance (A.14)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.			
A.14.2.2 *System change control procedures*	Visma e-conomic has defined a system change control procedure, which is supported by workflows in the change management system, ensuring that each step is documented.	Deloitte inspected that a system change control procedure is in place. Deloitte inspected documentation for a sample of changes that the change management flow was implemented and documented in accordance with the procedure.	No exceptions noted.
A.14.2.3 *Technical review of applications after operating platform changes*	Changes to e-conomic are tested in order to ensure that the change does not affect the operation or the security.	Deloitte inspected that a procedure for technical review of applications after operating platform changes is in place. Deloitte inspected documentation for a sample of changes and assessed that it successfully passed the tests before implementation.	No exceptions noted.
A.14.2.8 *System security testing*	Visma e-conomic has established procedures for securing functionality testing during development for e-conomic.	Deloitte inspected the procedures for security testing related to development tasks. Deloitte inspected documentation, for a sample of changes, showing that the changes have been formally tested and approved before the changes are moved to the live environment.	No exceptions noted.

4.4.8 Supplier service delivery management (A.15)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.2.1 *Monitoring and review of supplier services*	Visma e-conomic has established a process to monitor and review supplier services. Visma e-conomic is monitoring and reviewing supplier services delivery on a regular basis.	Deloitte inquired with key personnel whether processes are in place for monitoring and reviewing supplier services. Deloitte inspected the process for monitoring and reviewing supplier services. Deloitte inspected SOC2 Audit reports for a selected sample of suppliers.	No exceptions noted.

4.4.9 Information security incident management (A.16)

Control Area	Visma e-conomic's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.			
A.16.1.1 *Responsibilities and procedures*	Visma e-conomic has established a procedure in which managerial responsibilities for management of information security breaches are determined.	Deloitte inspected the procedures of information security incidents. Deloitte verified through inquiries that key personnel understand their tasks for information security incident breaches.	No exceptions noted.
A.16.1.2 *Reporting information security events*	Visma e-conomic has established a procedure to ensure that information security incidents are reported as quickly as possible.	Deloitte inspected the procedures of information security incidents. Deloitte inspected documentation for a sample of information security events that information security incidents are reported in accordance with the procedure.	No exceptions noted.
A.16.1.5 *Response to information security incidents*	Visma e-conomic has established a procedure to ensure that information security incidents are reported in accordance with the documented procedures.	Deloitte inspected the procedures of information security incidents. Deloitte inspected documentation for a sample of information security events that information security incidents are reported in accordance with the procedure.	No exceptions noted.