



Visma e-conomic A/S

**ISAE 3402 type 1 Service Auditor's Report on General IT Controls
related to Visma e-conomic**

As of 5 November 2019

Table of Contents

1	Independent Service Auditor's Report	1
2	Visma e-conomic A/S's assertion	3
3	Visma e-conomic A/S's description	4
4	Controls, control objectives, tests and results of hereof	12

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-economic A/S, Visma e-economic A/S's customers and their auditors.

Scope

We have been engaged to report on Visma e-economic A/S's (henceforth "Visma") description in section 3 of its e-economic system for processing customers' transactions as of 5 November 2019 (the description), and on the design, and implementation of controls related to the control objectives stated in the description.

Visma uses the subservice providers Google Cloud Platform, Amazon Web Services and Microsoft Azure to perform general IT controls around production environment for storage and hosting of data, network, infrastructure, application and database servers. Visma'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'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. The opinion does not include the suitability of the design and operating effectiveness of these complementary controls.

Visma's Responsibilities

Visma 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'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 and design 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. 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'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'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.

Basis for Qualified Opinion

We have noted a control deficiency in design and implementation of a control related to monitoring and review of supplier services. This resulted in the non-achievement of the control objective "A15 Supplier service delivery management: Maintain an agreed level of information security and service delivery in line with supplier agreements." as of 5 November 2019.

Qualified 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, except for the matter described in the Basis for Qualified Opinion paragraph:

- (a) The description of the general IT controls related to the e-economic system fairly presents, in all material respects, the controls as they were designed and implemented as of 5 November 2019; and
- (b) The controls related to the control objectives stated in the description were suitably designed and implemented as of 5 November 2019.

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 the e-economic system, 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, 14 February 2020

Deloitte

Statsautoriseret Revisionspartnerselskab



Thomas Kühn

Partner, State-Authorised Public Accountant

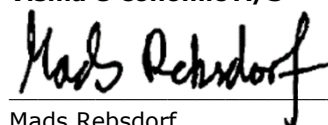
2 Visma e-conomic A/S's assertion

The accompanying description has been prepared for customers who have used the e-conomic system 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 confirms that:

- a) The accompanying description in section 3 fairly presents e-conomic system for processing customers' transactions as of 5 November 2019. 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 transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions 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 transactions.
 - 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. 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 as of 5 November 2019. 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.

Copenhagen, 14 February 2020

Visma e-conomic A/S



Mads Rebsdorf
Managing Director

3 Visma e-economic A/S's description

3.1 Introduction

This report is designed to provide information to be used by Visma e-economic A/S's clients and their auditors. This report has been prepared to provide information on the general IT controls applicable to the e-economic solution provided by Visma e-economic A/S. Application controls in e-economic are not covered in this report.

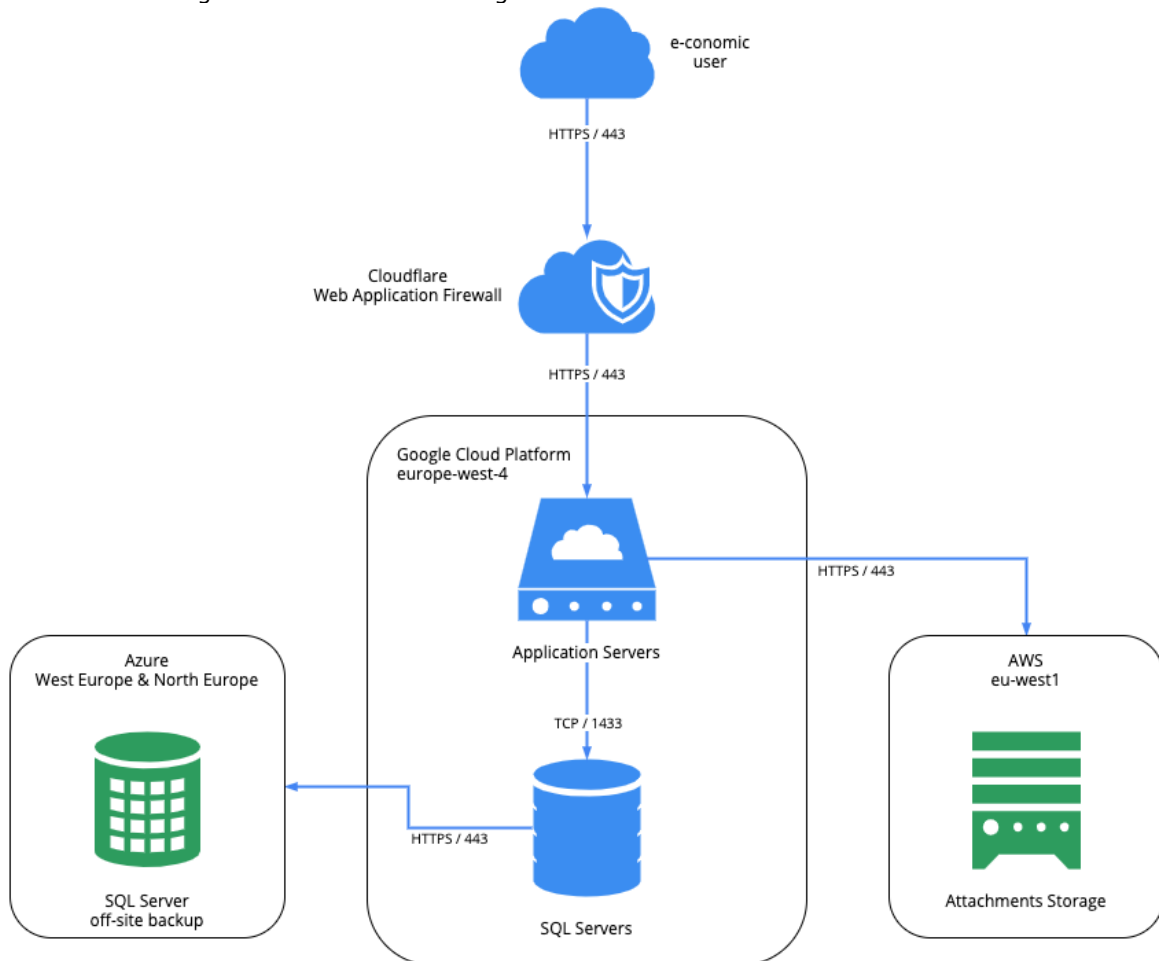
3.2 Description of Visma e-economic A/S's services

Visma e-economic A/S is a software company selling cloud-based solutions within the areas of ERP, electronic invoicing, and accounting to the Danish Market.

3.3 e-economic

E-economic is a cloud-based accounting system, developed and offered by Visma e-economic A/S that enables small and medium sized businesses to operate their accounting and bookkeeping practices as expected by Danish law. Via integrations to third-party applications such as time management tools, booking systems, and inventory management software, it is possible to achieve an all-round administration solution for a business. Furthermore, it is possible to upscale the system to have ERP functionalities.

The e-economic solution is utilizing 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.



3.4 Security governance in Visma and Visma e-economic

The CEO of Visma Group is overall accountable for information security.

Responsibility for information security is a line responsibility and distributed in the organisation.

3.4.1 All employees

All employees are responsible for following general security policies and the security provisions of their roles and the procedures they perform.

It is the collected practices of all Visma employees that contribute 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. It is therefore every employee's responsibility to follow the policies and procedures of Visma.

Security incidents and violations of Visma security policies should be reported to the nearest manager.

All employees are encouraged to suggest improvements to the security policies if the policies are inadequate.

3.4.2 Managers

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

3.4.3 Visma Security Forum

Visma Security Forum consists of Security Professionals that represent business units in various parts of Visma Group.

The Security Forum has mandate to suggest security policy on Visma Group level to management, including policy on access and usage of common infrastructure and services. Policies are approved by Visma Group Management. Published policies will be reviewed and updated at least annually.

Policy will only be set on Visma Group level when there is consensus among the divisions. In all other cases, policy will be set on division or entity level.

The Visma e-economic team follows the general rules from Visma Group. All new members of the Visma e-economic team will be introduced to the security rules and behaviour in Visma through the onboarding process in the beginning of their employment in Visma e-economic.

3.5 Control environment

In support of delivering e-economic, Visma has established the following general IT controls (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).

3.6 Information security policy (A.5)

3.6.1 Policies for information security

The information security policies in Visma e-conomic are developed and maintained by the Visma Security Forum and as a minimum on an annual basis approved by the Visma group management team as well as the management team of Visma e-conomic.

The Security Policy is available on the intranet for all employees and new employees will be made aware of the policy as part of the onboarding process

3.6.2 Risk Management

A prerequisite for efficient risk management is an open-eyed identification of the risks associated with Visma e-conomic operations and an explicit recognition of unacceptable risk.

The objective of Visma e-conomic security work is to identify all relevant risks, eliminate unnecessary risks and control unavoidable risks so the collected risk level is kept at an acceptable level, while ensuring that information systems and work procedures remain efficient.

The information security of Visma e-conomic is determined by the risk awareness of Visma employees and by the collected protection provided by all deployed controls (i.e. policies, procedures, standards, guidelines and systems) that contribute to the confidentiality, integrity and availability of critical information.

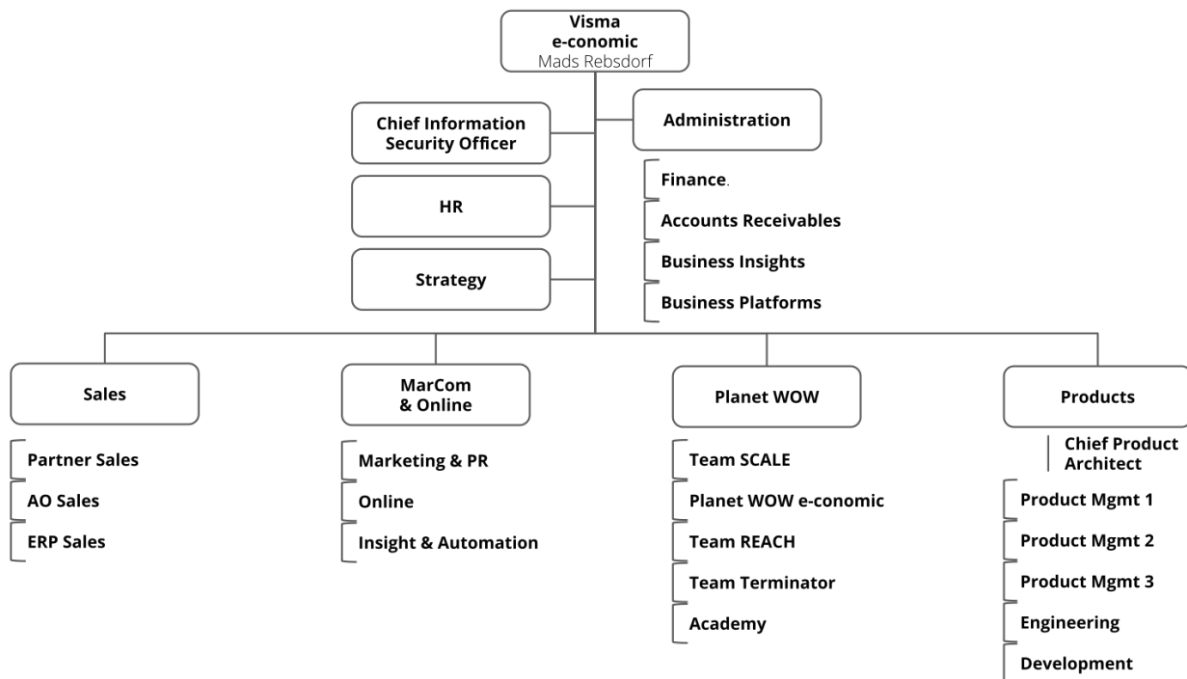
Risk assessment of the e-conomic application and its components is performed on an annual basis. The result of the risk assessment is documented in an internal list. The list must be approved by the Visma Product Security unit.

3.7 Internal organisation (A.6)

3.7.1 Information security roles and responsibilities

The management of Visma e-conomic has defined and allocated all information security responsibilities, appointed a Chief Information Security Officer, and established an Information Security Board.

Please see the current organisation structure as of 1 November 2019.



Furthermore, Visma e-economic is utilizing the Quality Management roles defined by the Visma Group to ensure segregation of duties and limit access to production data.

In case of a security breach, Visma e-economic will work closely together with the Cyber Security Incident Response Team (CSIRT) in the Visma Group.

3.8 Human resources security (A.7)

3.8.1 Screening

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

Depending on the role and responsibilities the candidate is to take on, there might be more gates for the candidate to pass before reaching the final phase and to be offered a contract. These include reference calls, and for employees who will have access to the production database, it is required that they have no criminal records. Finally, all employment contracts include a non-disclosure agreement covering information related to customer data, sales and marketing data, strategy and other confidential business data.

3.8.2 Information Security awareness, education and training

The assets of Visma e-economic include our employees and we ensure that our employees receive continuous training. This is done by sharing internal knowledge, relevant external courses and certifications. All new Visma e-economic employees will participate in an information security onboarding session.

3.9 Access control (A.9)

3.9.1 Access control policy

Visma e-economic ensures that access to information and information processing facilities is limited. The Access control policy is based on a 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.

3.9.2 User access provisioning

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

3.9.3 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.

3.9.4 Removal or adjustment of access rights

Upon employee role changes or terminations, Visma Group centrally handles off-boarding from central systems. For any systems not controlled centrally, Visma e-conomic A/S uses an off-boarding checklist.

3.9.5 Secure log-on procedures

Password requirements are described in the security policy. User passwords must meet the length and complexity requirements, and MFA should be used where supported. Systems which do not support Multi Factor Authentication (MFA) require the user to change the password every 90 days.

3.9.6 Password management system

Visma e-conomic uses a password management system where we enforce strong master passwords and MFA.

3.10 Operations security (A.12)

3.10.1 Documented operating procedures

Visma e-conomic 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 environments.

DevOps Field Guides contain information about essential areas of daily operations. Incidents are collected from various tools and sent to an alerting system that alerts relevant people. After an incident, a post-mortem is held.

3.10.2 Change management

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

3.10.3 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.

3.10.4 Separation of development, testing and operational environments

Development, testing and operational environments are completely separate from each other. Only operations personnel have access to deploy to production. Developers have read access to see status of deployments.

3.10.5 Information backup

Information saved in databases is protected by means of everyday backup to the local disk and it is subsequently copied to the external storage. The backup retention period is 90 days on the external storage.

Also, transaction log backups are performed frequently for point-in-time recovery. Finally, restore test of the production database is performed on a daily basis.

3.10.6 Event logging

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

3.10.7 Protection of log information

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

3.10.8 Installation of software on operational systems

Visma e-economic performs a weekly build of the base application image based on the most recent images available with our cloud vendor. 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 development, test and production environments.

3.10.9 Management of technical vulnerabilities

Visma e-economic minimizes the risk of exploitation of technical vulnerabilities by an effective patch procedure as well as regular vulnerability scans of the code base as well as of the infrastructure.

3.11 Communications security (A.13)

3.11.1 Network controls

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

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

3.12.1 System change control procedures

Visma e-economic ensures that information systems are designed and implemented according to the system development and security life cycle, which ensures 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 prioritized in the Product Steering Group.

For some projects, a Project Mandate will be 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.

3.12.2 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.

3.12.3 System security testing

Our development principles secure a high quality through the following steps:

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

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

3.13 Supplier relationships (A.15)

3.13.1 Monitoring and review of supplier services

A process for supplier acceptance has been established to ensure classification of suppliers and, if applicable, to ensure supplier acceptance of security requirements.

Visma e-economic 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.

3.14 Information security incident management (A.16)

3.14.1 Responsibilities and procedures

Visma e-economic 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.

All employees are also required to stay updated with the help of support websites, discussion forums, respond to alarms from our systems and customers, partners, etc. to detect weaknesses.

3.14.2 Reporting information security events

Reported information security or privacy events and weaknesses are reviewed and classified on a regular basis.

3.15 Complementary user entity controls

The e-conomic solution is designed on the assumption that certain controls would be implemented and operated effectively by the customer.

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

The list below describes additional controls that should be in operation in customer organisation to complement the controls at Visma e-conomic.

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

The customers should consider whether the following complementary controls have been implemented and operated effectively at the user organisations:

- Controls to ensure that physical access to the customers' premises is restricted to authorized individuals.
- Controls to ensure that the customer organisation has proper control over the use of IDs and passwords that are used for accessing information in the e-conomic solution.
- Controls to ensure that the access rights assignments for the e-conomic solution are provided adequately and in compliance with the user's work-related needs.
- Controls to ensure that the customer organisation takes action on access in case of resignations, retirements, or job rotations.
- Change management processes related to configuration changes, including controls to ensure that configuration changes are authorized, tested and approved.

4 Controls, control objectives, tests and results hereof

4.1 Introduction

This report is intended to provide Visma’s customers with information about the controls at Visma for economic that may affect the processing of user organisations’ transactions and also to provide Visma’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.

Our testing of Visma’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’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
<i>Inquiry</i>	Interview, i.e., inquiry with selected personnel at Visma
<i>Observation</i>	Observation of the execution of control
<i>Inspection</i>	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.
<i>Re-performance of control</i>	Repetition of the relevant control to verify that the control functions as intended.

4.3 Test of Design and Implementation

Our test of the design and implementation of controls includes such tests as we consider necessary to assess 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 as of 5 November 2019.

4.4 Control objectives, controls, and test results

4.4.1 Information Security Policy (A.5)

Control Area	Visma'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 <i>Policies for information security</i>	Visma 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 <i>Risk assessment</i>	Visma 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 <i>Review of the policies for information security</i>	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 was approved by management.	No exceptions noted.

4.4.2 Organisation of Information Security (A.6)

Control Area	Visma'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 <i>Information security roles and responsibilities</i>	Visma 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'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 <i>Screening</i>	<p>Visma 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.</p> <p>For employees with access to customer systems and data, a criminal record is obtained prior to the recruitment of the candidate.</p> <p>All employment contracts include a non-disclosure agreement covering information related to confidential business data.</p>	<p>Deloitte inspected the procedures used and the procedures performed for screening.</p> <p>Deloitte inquired with key personnel about the process for screening.</p> <p>Deloitte inquired with key personnel about the process for signing non-disclosure agreements.</p>	<p>We have not been able to test procedures, since we have been informed that no employments to the DevOps-function have occurred during 2019.</p> <p>No further exceptions noted.</p>
A.7.2.2 <i>Information security awareness, education and training</i>	<p>Visma conducts training related to information security through onboarding sessions with new employees.</p>	<p>Deloitte inspected the latest training material used for training of new employees.</p>	<p>No exceptions noted.</p>

4.4.4 Access control (A.9)

Control Area	Visma's control activity	Test performed by Deloitte	Test Results
Control objective: To limit access to information and information processing facilities.			
A.9.1.1 <i>Access control policy</i>	<p>An access control policy is established, documented and reviewed based on business and information security requirements.</p>	<p>Deloitte inspected that an access control policy is established.</p> <p>Deloitte verified for one sample that access to e-conomic has been granted in accordance with the implemented policy.</p>	<p>No exceptions noted.</p>

Control Area	Visma's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
A.9.2.2 <i>User access provisioning</i>	<p>A formal user access procedure is implemented to ensure that access rights are allocated based on position and department.</p> <p>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.</p> <p>Requests are approved by immediate manager.</p>	<p>Deloitte inspected that a procedure for user provisioning is in place.</p> <p>Deloitte observed that a system is used for user access provisioning.</p> <p>Deloitte verified for one sample that the process for time-based access has been implemented in accordance with the procedure.</p>	No exceptions noted.
A.9.2.5 <i>Review of user access rights</i>	<p>Users and their access rights for internal systems and client data are reviewed on a regular basis by immediate manager to prevent unauthorised access to systems and services.</p>	<p>Deloitte inspected the procedures for review of users and user access rights.</p> <p>Deloitte assessed the latest performed review.</p>	No exceptions noted.
A.9.2.6 <i>Removal or adjustment of access rights</i>	<p>Visma 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.</p>	<p>Deloitte inspected the procedures for removal or adjustment of access rights.</p> <p>Deloitte verified for one sample that the process for closing down users has been implemented in accordance with the procedure.</p>	No exceptions noted.
Control objective: To prevent unauthorized access to systems and applications.			
A.9.4.2 <i>Secure log-on procedures</i>	<p>A password policy has been established in Visma's information security policy.</p> <p>Passwords are configured as follows.</p> <ul style="list-style-type: none"> • 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. 	<p>Deloitte inspected the procedures for use of passwords.</p> <p>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.</p> <p>Deloitte inspected that administrative passwords are handled through the password tool '1password'.</p>	No exceptions noted.

Control Area	Visma's control activity	Test performed by Deloitte	Test Results
A.9.4.3 <i>Password management system</i>	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 sample basis, Deloitte inspected '1password' in order to ensure storage of passwords, access and password requirements.	No exceptions noted.

4.4.5 Operations security (A.12)

Control Area	Visma'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 <i>Documented operation procedures</i>	Visma 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 <i>Change management</i>	Visma 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 verified for one sample that the process for change management has been implemented in accordance with the procedure.	No exceptions noted.
A.12.1.3 <i>Capacity management</i>	Visma has implemented a process for capacity management, which is supported by various tools to monitor capacity and operational errors. Visma 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 e-conomic status page showing incident reporting to customers regarding capacity monitoring.	No exceptions noted.

Control Area	Visma's control activity	Test performed by Deloitte	Test Results
A.12.1.4 <i>Separation of development, testing and operational environments</i>	Visma 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 <i>Information backup</i>	<p>Visma has established backup procedures for economic.</p> <p>Restoration of data from backup systems is tested regularly.</p> <p>Backups are stored locally as well as externally at another geographical and secure location.</p>	<p>Deloitte inspected the backup procedures to assess whether backup procedures are adequate.</p> <p>Deloitte inspected documentation regarding the backup configurations to assess whether these are implemented in accordance with the backup procedures.</p> <p>Deloitte verified for one sample that restore from backup has been performed in accordance with the procedure.</p>	No exceptions noted.
Control objective: To record events and generate evidence.			
A.12.4.1 <i>Event logging</i>	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.	<p>Deloitte assessed the log mechanisms and procedures regarding security logging in general.</p> <p>Deloitte inspected a sample of one user log to verify that user access is logged.</p>	<p>We have noted that no formal procedure is in place to ensure that logs are proactively reviewed. We have been informed that logs are reviewed upon errors and troubleshooting.</p> <p>No further exceptions noted.</p>
A.12.4.2 <i>Protection of log information</i>	<p>Logging facilities are protected from unauthorised access by the security measures established on the servers.</p> <p>Access to log information is limited by the operating system's user control on the machines where data is stored.</p> <p>Access to log information is granted by time-based tokens and is restricted with view access.</p>	<p>Deloitte inquired with key personnel whether procedures are in place for safeguarding logs.</p> <p>On a sample basis, Deloitte has inspected that only employees with a work-related need have access to the logs.</p> <p>Deloitte verified for one sample that the process for time-based access has been implemented in accordance with the procedure.</p>	No exceptions noted.

Control Area	Visma's control activity	Test performed by Deloitte	Test Results
Control objective: To ensure the integrity of operational systems.			
A.12.5.1 <i>Installation of software on operational systems</i>	Software installations on operating software is 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 verified for one sample that the installation and upgrade are performed in accordance with the procedure.	No exceptions noted.
Control objective: To prevent exploitation of technical vulnerabilities.			
A.12.6.1 <i>Management of technical vulnerabilities</i>	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 the latest vulnerability scan 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'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 <i>Network controls</i>	Visma 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 verified for one sample that changes to network infrastructure has been reviewed and approved by peer review prior to deployment.	No exceptions noted.

Control Area	Visma's control activity	Test performed by Deloitte	Test Results
A.13.1.3 <i>Segregation in networks</i>	<p>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.</p> <p>Visma has segregated the network into subnets covering internal-, staging-, sandbox- and production environments.</p>	<p>Deloitte inspected the segregation of networks and verified that access to the wireless network requires a username and a password.</p> <p>Deloitte inspected documentation for the segregation of networks in subnets.</p>	No exceptions noted.

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

Control Area	Visma'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 <i>System change control procedures</i>	Visma has defined a system change control procedure, which is supported by workflows in the change management system, ensuring that each step is documented.	<p>Deloitte inspected that a system change control procedure is in place.</p> <p>Deloitte verified for one sample that the change management flow was implemented and documented in accordance with the procedure.</p>	No exceptions noted.
A.14.2.3 <i>Technical review of applications after operating platform changes</i>	Changes to e-conomic are tested in order to ensure that the change does not affect the operation or the security.	<p>Deloitte inspected that a procedure for technical review of applications after operating platform changes is in place.</p> <p>Deloitte inspected documentation for one change and assessed that it successfully passed the tests before implementation.</p>	No exceptions noted.
A.14.2.8 <i>System security testing</i>	Visma has established procedures for securing functionality testing during development for e-conomic.	<p>Deloitte inspected the procedures for security testing related to development tasks.</p> <p>Deloitte verified for one sample that the change has been formally tested and approved before the change is moved to the live environment.</p>	No exceptions noted.

4.4.8 Supplier service delivery management (A.15)

Control Area	Visma'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.			
<i>A.15.2.1 Monitoring and review of supplier services</i>	<p>Visma has established a process to monitor and review supplier services.</p> <p>Visma is monitoring and reviewing supplier services delivery on a regular basis.</p>	<p>Deloitte inquired with key personnel whether processes are in place for monitoring and reviewing supplier services.</p> <p>Deloitte inspected ISO 27001 certificates for a selected sample of suppliers.</p>	<p>We have noted that the process for monitoring and reviewing supplier services has not been sufficiently documented.</p> <p>No further exceptions noted.</p>

4.4.9 Information security incident management (A.16)

Control Area	Visma'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.			
<i>A.16.1.1 Responsibilities and procedures</i>	<p>Visma has established a procedure in which managerial responsibilities for management of information security breaches are determined.</p>	<p>Deloitte inspected the procedures of information security incidents.</p> <p>Deloitte verified through inquiries that key personnel understand their tasks for information security incident breaches.</p>	<p>No exceptions noted.</p>
<i>A.16.1.2 Reporting information security events</i>	<p>Visma has established a procedure to ensure that information security incidents are reported as quickly as possible.</p>	<p>Deloitte inspected the procedures of information security incidents.</p> <p>Deloitte verified for one sample that information security incidents are reported in accordance with the procedure.</p>	<p>No exceptions noted.</p>
<i>A.16.1.5 Response to information security incidents</i>	<p>Visma has established a procedure to ensure that information security incidents are reported in accordance with the documented procedures.</p>	<p>Deloitte inspected the procedures of information security incidents.</p> <p>Deloitte verified for one sample that information security incidents are reported in accordance with the procedure.</p>	<p>No exceptions noted.</p>