

# Visma e-conomic a/s

## ISAE 3402 type 2 assurance report

in relation to general IT controls for e-conomic online  
accounting system for the period 1 December 2016 to 30  
November 2017





## Contents

1	e-conomic online accounting system	2
1.1	Introduction	2
1.2	Server management	2
1.3	System set-up	2
1.4	Use of subservice organisation	4
1.5	Complementary user entity controls	4
2	Visma e-conomic a/s' Management statement for the period 1 December 2016 to 30 November 2017	5
3	Independent auditor's assurance report on the description of controls, their design and operating effectiveness regarding e-conomic online accounting system for the period 1 December 2016 to 30 November 2017	6
4	Tests performed by EY	8
4.1	Objective and scope	8
4.2	Tests performed	8
4.3	Controls and tests performed by EY	9

## 1 e-conomic online accounting system

### 1.1 Introduction

e-conomic is an online accounting system used by more than 100,000 companies.

This service auditor's assurance report is related to general IT controls at Visma e-conomic a/s regarding the e-conomic online accounting system.

The general IT controls covered by this report have been tested at Visma e-conomic a/s covering the global e-conomic solution.

The process at Visma e-conomic a/s regarding general IT controls is:

- ▶ Server management
- ▶ System set-up:
  - System documentation and changes to data
  - Customer access
  - Development and personal access to production environment
  - Incident management

### 1.2 Server management

Management of hosted server

Control objective: Controls which provide reasonable assurance that the management of hosted servers secure the operation of e-conomic online accounting system and that the security level is following the agreed standards.

The servers in Visma e-conomic a/s' production environment are housed at a sourcing partner but primarily maintained by Visma e-conomic a/s.

All servers are patched according to an existing patch plan, which includes software, service windows and coordination with the sourcing partner regarding patch management of infrastructure (1.1).

The e-conomic production environment is monitored 24/7 and includes predefined thresholds as regards availability and response time. If a threshold is triggered, an automated alert will follow an escalation process to ensure that all incidents are resolved in a timely manner (1.2 and 1.3).

The backup procedures supporting the production environment include constant data mirroring and storage in high security facilities (1.4).

Offline backup procedures have been implemented to minimise any risk of loss of data (1.5 to 1.7).

Visma e-conomic a/s has implemented continuity plans in cooperation with their sourcing partner which include frequent restores of the production environment to ensure a reliable plan (1.8).

### 1.3 System set-up

System documentation and changes to data

e-conomic system set-up, system documentation and changes to data

Control objective: Controls provide reasonable assurance that the system set-up ensures that the daily operations comply with requirements regarding system documentation and changes to data.

Within e-conomic online accounting system, logging of changes to all selected master data is established (2.1).

Visma e-conomic a/s has a procedure to handle requests from users to make corrections in their data. The procedure requires that the customer formally requests the change and subsequently approves the change (2.2).

Visma e-conomic a/s continually updates the user documentation for e-conomic online accounting system. The current user documentation is always available under e-copedia from the e-conomic website (2.3).

#### Customer access

##### e-conomic system set-up, customer access

Control objective: Controls provide reasonable assurance that the system set-up provides secure access to the e-conomic online accounting system and facilities to limit access to accounting data on a user basis.

All use of the e-conomic online accounting system is performed in a secure way through an encrypted SSL connection with a minimum of 128 bits encryption (3.1).

In order for users to log on to the e-conomic online accounting system, they are required to use a login system consisting of an agreement number, personal user name and personal password. User name and password can be changed within the system (3.2).

Within the system, the superuser of each customer can change the access rights of users within the company (3.3).

The e-conomic accounting system is designed in such a way that data for customers are separated based on the agreement number (3.4). There are controls to verify the customers prior to resetting or changing the password and/or e-mail to the customer superuser account in the e-conomic application (3.5).

#### Development and personal access to production environment

##### e-conomic system set-up, development and personal access to e-conomic production environment

Control objective: Controls provide reasonable assurance that system development is authorised, tested and approved before implemented in the production system. Further, access controls to the production environment secure that only authorised personnel has access to the production environment.

All high level roadmap development activities are authorised at a steering group meeting. A Steering group meeting is held when changes to the Roadmap is approved. (4.1).

Visma e-conomic a/s has a procedure regarding development and maintenance of the system once a week it is agreed, which functions should be added or updated. After this has been decided, the process regarding development, review, test and approval is started. The entire cycle lasts approximately two weeks (4.1 and 4.4).

Prior to initiating development of new functionalities, a pull request is made for the relevant part of the source code that would be affected (4.2).

Changes are transferred to a public cloud where tests, peer review and QA are performed. After completed tests and peer review, the changes are transferred to staging environment (4.3).

Weekly completed changes are reviewed and accepted. After business accept of the change, these are pushed to production environment in two stages (4.4).

Development to the application is authorised, tested, approved and documented before being implemented in the system. If errors occur when changes have been implemented, an analysis of the root cause for the errors is performed, and actions are taken to prevent similar errors again (post-mortem report) (4.5).

All emergency changes of the system caused by fixes of critical bugs are afterwards passed through the same approval procedures as normal system development (4.6).

Visma e-conomic a/s enforces strong access restrictions to their production environment which include meticulous user administration and regular reviews. Any internal access is restricted to specific functions (4.7 to 4.9).

The production environment is protected by password policies and procedures to ensure a secure platform (4.10).

All relevant user activity is logged through comprehensive and secured logs (4.11).

The system documentation is automatically updated after implementing changes (4.12).

#### Incident management

e-conomic system set-up, incident management

Control objective: Controls provide reasonable assurance that the system set-up ensures that all problems are identified, recorded, analysed and resolved.

Visma e-conomic a/s has a procedure where incidents either reported from alerts within the system or incidents or problems reported by users are flagged, relevant personnel is notified, and a solution is initiated within 24 hours or less. (5.1).

All problems and errors are tracked and prioritised. Problem trends are monitored (5.2).

#### 1.4 Use of subservice organisation

Visma e-conomic a/s uses Sentia A/S as subservice organisation. The services delivered by Sentia A/S are primarily limited to physical hosting of the servers of the e-conomic online accounting system and storage of backups performed by Visma e-conomic a/s.

Controls at Solido are not included in this report and are therefore carved out.

#### 1.5 Complementary user entity controls

The e-conomic online accounting system is designed based on effective controls at the user entities. These controls are necessary to achieve the control objectives stated by Visma e-conomic a/s.

In order to achieve the stated control objectives, the following key controls should be implemented and be effective at the user entities:

##### Customer access

Administration of users' access and segregation of duties within the e-conomic online accounting system.

##### Physical security

Physical security at the user entity, ensuring security for the client computers using the e-conomic online accounting system.

2 Visma e-conomic a/s' Management statement for the period 1 December 2016 to 30 November 2017

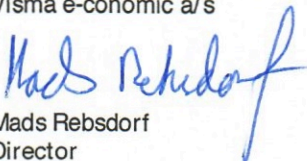
The accompanying description has been prepared for Visma e-conomic a/s' customers who have used the "e-conomic online accounting system" and their auditors who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves when assessing the risks of material misstatements of customers' financial statements.

Visma e-conomic a/s uses the subservice organisation Sentia A/S for physical hosting and network management. This report does not include controls operated by Sentia A/S.

Visma e-conomic a/s confirms that:

- (a) The description in Section 1 fairly presents the general IT controls supporting the e-conomic online accounting system throughout the period 1 December 2016 to 30 November 2017. The criteria used in making this statement were that the accompanying description:
  - (i) Presents how the general IT controls were designed and implemented, including:
    - ▶ The types of services provided.
    - ▶ How the system dealt with significant events and conditions, other than transactions.
    - ▶ The process used to operate the general IT controls.
    - ▶ 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 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, communication, control activities and monitoring controls that were relevant to the general IT controls.
  - (ii) Includes relevant details of changes to the service organisation's system during the period 1 December 2016 to 30 November 2017.
  - (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 and operated effectively throughout the period 1 December 2016 to 30 November 2017. The criteria used in making this statement were that:
  - (i) the risks that threatened achievement of the control objectives stated in the description were identified; and
  - (ii) the identified controls would, if operated as described, provide reasonable assurance that the risks did not prevent the stated control objectives from being achieved; and
  - (iii) the controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period 1 December 2015 to 30 November 2017.

Copenhagen, 7 March 2018  
Visma e-conomic a/s



Mads Rebsdorf  
Director

### 3 Independent auditor's assurance report on the description of controls, their design and operating effectiveness regarding the e-conomic online accounting system for the period 1 December 2016 to 30 November 2017

To Management of Visma e-conomic a/s

#### Scope

We have been engaged to report on Visma e-conomic a/s' description in Section 1 of the general IT controls supporting e-conomic online accounting system for processing customers' transactions throughout the period 1 December 2016 to 30 November 2017 (the description) and on the design and operation of controls related to the control objectives stated in the description. The general IT controls included in this report have been tested at Visma e-conomic a/s covering the global e-conomic solution.

Management's description of controls does not include control objectives and associated controls at the subservice organisation Sentia A/S. This report is prepared as carve-out for the subservice organisation, and our testing does not include controls operated by Sentia A/S.

#### Visma e-conomic a/s' responsibility

Visma e-conomic a/s is responsible for: preparing the description and accompanying statement in Section 2, including the completeness, accuracy and method of presentation of the description and the statement; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

#### Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, as well as FSR –Danish Auditors' guidelines for ethical conduct of Auditor based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

Ernst & Young Godkendt Revisionspartnerselskab applies International Standard on Quality Control, ISQC 11 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

#### Auditor's responsibility

Our responsibility is to express an opinion on Visma e-conomic a/s' description and on the design and operation 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 Organizations", and additional requirements under Danish Audit legislation in order to obtain reasonable assurance for our opinion. That standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures including testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by Visma e-conomic a/s and described in Section 2.

---

1 ISQC 1, Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance and Related Services Engagements

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 a/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. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk and that controls at a service organisation may become inadequate or fail.

#### Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in Section 1. In our opinion, in all material respects:

- (a) the description fairly presents the general IT controls supporting the e-conomic online accounting system as designed and implemented throughout the period from 1 December 2016 to 30 November 2017; and
- (b) the controls related to the control objectives stated in the description were suitably designed throughout the period from 1 December 2016 to 30 November 2017; 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 December 2016 to 30 November 2017.

#### Description of tests of controls

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

Copenhagen, 7 March 2018  
Ernst & Young  
Godkendt Revisionspartnerselskab  
CVR no. 30 70 02 28



Claus Andersen  
Partner



Nils B. Christiansen  
State Authorised  
Public Accountant  
MNE-no.: mne34106



## 4 Tests performed by EY

### 4.1 Objective and scope

We conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organization.

Our tests of design and operating efficiency of controls throughout the period 1 December 2016 to 30 November 2017 have been performed on a sample basis and comprised the control objectives and related controls which have been selected by Management as stated in Section 4.3 below. The general IT controls have been tested at Visma e-conomic a/s covering the global e-conomic solution.

Any other control objectives, related controls and controls at connected financial enterprises are not covered by our tests.

### 4.2 Tests performed

Tests performed to evaluate design and implementation of controls at Visma e-conomic a/s regarding general IT controls are mentioned below.

Inspection	Inspection of documents and reports which contain specification of the performance of the control. This includes, for example, reading of and position taking to reports and other documentation in order to assess whether the specific controls have been designed so that these can be assumed to be effective if they are implemented. In addition, it is evaluated whether controls are monitored and controlled adequately and at suitable intervals.
Inquiries	Inquiry of appropriate personnel at Visma e-conomic a/s. Inquiries comprised questions regarding how controls are performed, documented and approved.
Observation	We have observed the performance of the control.
Re-performing control procedures	Repeat the relevant control. We have repeated the performance of the control to verify that the control is working as assumed.

### 4.3 Controls and tests performed by EY

Control objective – Management of hosted server			
1. Controls provide reasonable assurance that the management of hosted servers secure the operation of the e-conomic online accounting system and that the security level is following the agreed standards.			
No.	Control description	Tests performed by EY	Result of test of design and implementation
1.1	There is an existing patch plan where e-conomic servers are divided into two groups with different patch windows.	Inquired to the procedures for patching servers. Inspected the patch plan and latest patches installed on the servers.	Patch plan does not include requirements to frequency for patches. No patches have been installed since 5 May 2017 on domain controller. Except for this, no exceptions noted.
1.2	The e-conomic production environment is monitored 24/7 regarding availability and response time.	Inspected that the production environment is monitored 24/7 regarding availability and response time.	A new monitoring system was implemented on 1 March 2017, it has, therefore, not been possible to receive appropriate documentation for 24/7 monitoring between 1 December 2016 and 28 February 2017. Except for this, no exceptions noted.
1.3	Each monitor point is configured with its own threshold and grouped into severity levels with corresponding escalation processes.	Inspected the configuration, thresholds, grouping and escalation processes.	A new monitoring system was implemented on 1 March 2017, it has, therefore, not been possible to receive appropriate documentation for 24/7 monitoring between 1 December 2016 and 28 February 2017. Except for this, no exceptions noted.
1.4	All data is constantly mirrored and stored in high-security facilities on two different servers.	Inspected that all data is constantly mirrored. Inspected if servers are kept at different physical locations.	No exceptions noted.
1.5	At least every 15 minutes, a transaction log backup is created.	Inspected that a transaction log is backed up at least every 15 min.	No exceptions noted.
1.6	Every Friday night, a full database backup is created.	Inspected that a full backup of the production system is created every Friday.	No exceptions noted.

No.	Control description	Tests performed by EY	Result of test of design and implementation
1.7	All days but Friday, a differential database backup is created.	Inspected that differential database backups are created every day except Friday.	No exceptions noted.
1.8	Procedures for restoring the database are tested at least once a month.	Inspected that the main production database has been restored on a weekly basis.	No exception noted.

Control objective – e-conomic system set-up, system documentation and changes to data

2. Controls provide reasonable assurance that the system set-up ensures that the daily operations comply with requirements regarding system documentation and changes to data.

No.	Control description	Tests performed by EY	Result of test of design and implementation
2.1	Changes to all selected customer accounting data are logged by e-conomic.	Inquired to the procedure for logging of data by e-conomic. Inspected that changes to customer accounting data are logged.	No exceptions noted.
2.2	Correction of data is only performed on specific requests from customers after their approval. All corrections of data have to be approved by a DBA/Architect, and all corrections are reviewed by a DBA, Architect or 2 <sup>nd</sup> level supporter from e-conomic.	Observed on a sample basis that corrections of data are only performed upon request from customers, and all corrections are reviewed by a DBA, Architect or 2 <sup>nd</sup> level supporter.	It has not been possible to receive documentation for customers' approval in some cases. Except for this, no exceptions noted.
2.3	External documentation regarding the system can be accessed on all e-conomic websites under "e-copedia".	Observed that user documentation of e-conomic online accounting system is available from e-conomic's website.	No exceptions noted.

Control objective – e-conomic system set-up, customer access
3. Controls provide reasonable assurance that the system set-up provides secure access to the e-conomic online accounting system and facilities to limit access to accounting data on a user basis.

No.	Control description	Tests performed by EY	Result of test of design and implementation
3.1	The communication with the e-conomic application is secured by minimum 128-bit SSL encryption technology.	Inspected that the e-conomic online accounting system is hosted on servers using SSL certificates with minimum 128-bit encryption.	No exceptions noted.
3.2	Access to e-conomic is secured by a password-protected login system, with agreement number, personal user name and personal password.	Inspected that login to the e-conomic online accounting system requires use of agreement number, personal user name and personal password.	No exceptions noted.
3.3	Each user's access within the system can be limited at a function based level by granting them access to an area level.	Inspected that the user administration within the e-conomic online accounting system allows the super user to limit the user access within the application.	No exceptions noted.
3.4	All data is stored and logged on servers with a unique key which ensures segregation between customers.	Inspected that all data in the e-conomic online accounting system is associated with an agreement number. Inspected that customers can only access data associated with their own unique key.	No exceptions noted.
3.5	Customers are e-mail-verified before resetting the password to the customer user accounts in the e-conomic application.	Inquired to the procedure for resetting or changing the password to a customer user account. Observed a walk-through of how to reset a customer user account.	No exceptions noted.

Control objective – e-conomic system set-up, development and personal access to e-conomic production environment
4. Controls provide reasonable assurance that system development is authorised, tested and approved before implemented in the production system. Further, access controls to the production environment secure that only authorised personnel has access to the production environment.

No.	Control description	Tests performed by EY	Result of test of design and implementation
4.1	System Development Roadmap defines authorized system development. A Steering group meeting is held when changes to the Roadmap is approved.	Inquired to the procedure for development activities and authorisations. Inspected minutes from a steering group meeting approving changes to System Development Roadmap.	No exceptions noted.
4.2	Prior to initiating development of new functionalities, etc., a pull request is made of the relevant part of the effected source code.	Inquired to the procedure for development activities. Inspected a pull request including changes title, relevant part of the affected source codes and status of changes.	No exceptions noted.
4.3	Changes are transferred to a public cloud test server where tests, peer review and QA are performed.	Inquired to the procedure for development activities. Inspected that changes are tested and reviewed and QA is performed.	In 4 instances from a sample of 25 changes, the change was not peer reviewed prior to implementation and in 1 instance, the change was not tested. Except for this, no exceptions noted.
4.4	Changes are reviewed and accepted. After business accept of the change, these are pushed to production environment in two stages.	Inquired to the procedure for development activities. Inspected that changes are reviewed, accepted and pushed to production environment in two stages.	In 4 instances from a sample of 25 changes, the change was not reviewed prior to being pushed to production, and in 1 instance, the change was not approved before pushed to production. Except for this, no exceptions noted.
4.5	There is monitoring and traceability on who could push changes to production.	Inquired to the procedure for monitoring changes. Observed that a limited number of authorised people have the right to push changes to production. Inspected that only authorised people have pushed changed to production.	No exceptions noted.

4.6	Emergency changes are implemented immediately, but afterwards the changes undergo the same controls, tests and approvals as all other implementations in the system.	Inquired to the procedure for emergency changes. Inspected that emergency changes are approved, tested and implemented and that all have been documented.	No exceptions noted.
4.7	Accounts are divided into service accounts and personal accounts.	Observed that accounts are separated in service and personal accounts.	No exceptions noted.
4.8	Upon resignation or termination of employees, user accounts are disabled or locked, prohibiting access.	Inquired to the procedure for reviewing and updating personal accounts. Observed that personal accounts are updated according to the procedure.	No exceptions noted.
4.9	e-conomic employees who have access to the production data are limited to DBAs and technical 2 <sup>nd</sup> level support, and relevant activities are being logged.	Observed that employees with access to the production environment are limited to DBAs and technical 2 <sup>nd</sup> level support. Observed that logging is activated.	No exceptions noted.
4.10	e-conomic has a general password policy which is used.	Inspected the password policy requires: <ul style="list-style-type: none"> <li>▶ Enforced password history of five passwords remembered</li> <li>▶ Maximum password age of 90 days</li> <li>▶ Minimum password age of one day</li> <li>▶ At least eight characters in length</li> <li>▶ Complexity</li> </ul> Observed the implemented password policy.	No exceptions noted.
4.11	e-conomic is logging selected activities in the production environment.	Observed that selected activities in the production environment have been logged.	No exceptions noted.
4.12	Automatic controls are in place to update system documentation.	Observed that system documentation is automatically updated after changes.	No exceptions noted.

Control Objective – e-conomic system set-up, incident management
5. Controls provide reasonable assurance that the system set-up ensures that any problems are identified, recorded, analysed and resolved.

No.	Control description	Tests performed by EY	Result of test of design and implementation
5.1	Post Mortems are recorded, analysed and resolved. Resolution is initiated within 24 hours or less.	Inquired to the procedures for incident management. Observed that Post Mortems are recorded, analysed and resolved. Furthermore, we have observed that resolution is initiated within 24 hours or less.	No exceptions noted.
5.2	Problems and errors are tracked and prioritised. Trend of problems are monitored.	Inquired to the procedures for incident management. Observed problems and errors are tracked and prioritised. Furthermore, we have observed that problems and trend are monitored.	No exceptions noted.