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 2023 – 31 December 2023

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' (hereinafter "e-conomic") description in section 3 of its general IT controls related to the e-conomic application used by customers to process accounting data from 1 January 2023 to 31 December 2023 (the description). The scope of this report regards the design, implementation and operations of controls related to the control objectives stated in the description.

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

e-conomic's Responsibilities

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

Service Auditor's Responsibilities

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

We conducted our engagement in accordance with 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 and operating effectively.

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 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 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, 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

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.

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 that controls at a service organisation may become inadequate or fail.

Description of Tests of Controls

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

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 e-conomic application (e-conomic) fairly presents, in all material respects, the controls as they were designed and implemented throughout the period 1 January 2023 – 31 December 2023; and

(b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period 1 January 2023 – 31 December 2023; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2023 – 31 December 2023.

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.

This report is not intended to and should not be used by anyone other than the parties specified above.

Copenhagen, 23 January 2024

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. 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 2023 – 31 December 2023. 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 2023 to 31 December 2023.

   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.

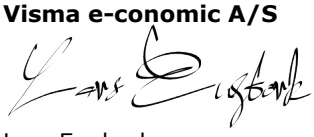
b) The controls related to the control objectives stated in the accompanying description were suitably designed, implemented and operated effectively in the period 1 January 2023 – 31 December 2023. The criteria used in making this assertion were that:

   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 2023 to 31 December 2023

Copenhagen, 23 January 2023

Visma e-conomic A/S



Lars Engbork
Managing Director

3 e-conomic's description

3.1 Introduction

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.

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 15,000 employees and 1.5 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, e-conomic is continuously working on improving its security and data protection procedures and practices throughout the organisation.

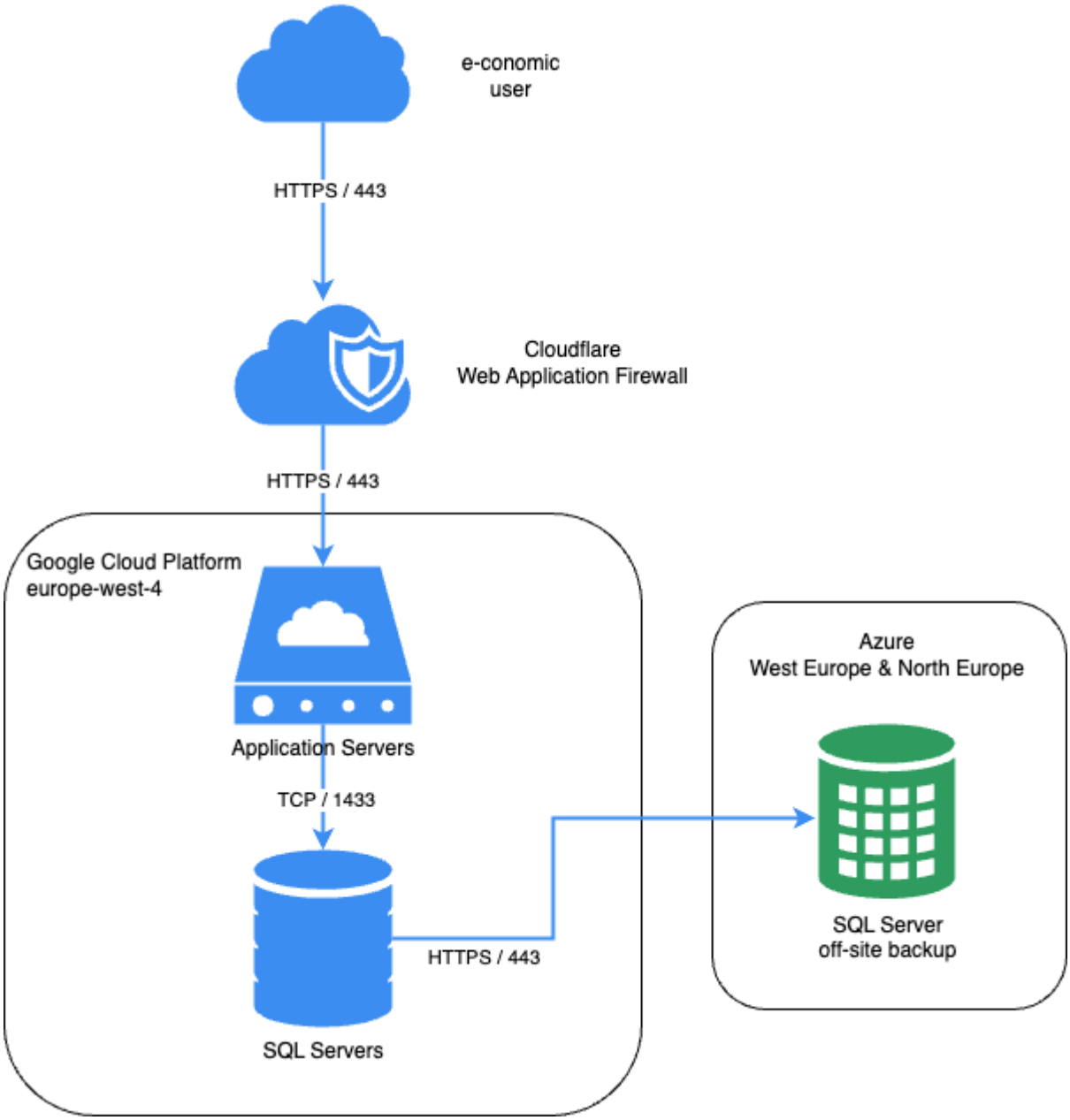
This report is designed to provide information to clients and auditors on the general IT controls applicable to the product, e-conomic. Application controls in e-conomic are not covered in this report.

3.2 Description of e-conomic's services

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 the e-conomic application, customers can handle accounting activities such as invoicing, sales, finance, bookkeeping, VAT accounts, financial 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, and Microsoft Azure for storage of database backups. Further, Cloudflare is used to provide web application firewalls and provides PKI for the encryption of our internet traffic and to verify server identity. This is illustrated in the high-level infrastructure diagram below.



3.3 Security governance in Visma Group and 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, e-conomic complies with the general policies and procedures set by Visma Group.

3.3.1 Visma Security Steering Group

The Visma Security Steering Group consists of the Visma CEO, Visma CISO, Visma DPO, and division directors. 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 program

- Align on emerging risk, business unit security and compliance issues.

3.3.2 e-conomic Security Forum

The e-conomic Security Forum consists of the Managing Director, Chief Product Architect, Director of Engineering, Head of Platform and Infrastructure, Director of Legal and Operations, Team Lead for the Identity and Security Teams and the Security Project Manager/Data Protection Manager.

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 e-conomic Security Forum maintains a risk register that is used to prioritise the mitigation and elimination of various security and privacy-related risks.

3.3.3 Security Champions and the Security Champions Guild

Within each product team, e-conomic appoints a Security Champion to be responsible for all security-related questions and issues in the application. Security Champions 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 Champions educate their colleagues in triaging security defaults and help conduct threat modelling in their teams.

The Security Champions meet monthly to discuss and escalate various security issues within the various teams.

3.3.4 Managers

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

3.3.5 All employees

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

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 e-conomic's security policies to their nearest manager or the Security team. All employees are encouraged to suggest improvements to the security policies if the policies are inadequate.

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

3.4 Control environment

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

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, 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
- Mobile device and Removable storage
- Email security
- Remote access
- Working in public areas
- Personal computer management
- Information classification and handling

The Visma Information Security Policy is implemented throughout e-conomic in addition to other security policies tailored to fit the practices of 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 e-conomic, 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, e-conomic uses the *risk = impact x likelihood* methodology, with risk, impact and likelihood levels appropriate to 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, e-conomic is able to maintain an acceptable level of risk through the implementation of technical and organisational controls.

Risk management at e-conomic is implemented on multiple levels. On a high level, the 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 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 e-conomic.

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.

In relation to third-party providers, Visma has implemented a Vendor Management Framework. As part of the framework, all third parties that process personal data on behalf of e-conomic and its customers are subject to ongoing assessments. 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, the level of encryption and deletion procedures. Based on these assessments, risks are identified and assessed by e-conomic. For third parties that process data outside of the EU/EEA, risks are identified for the processing of data in third countries.

3.6 Internal organisation (A.6)

3.6.1 Information security roles and responsibilities

As a part of Visma Group, e-conomic complies with the policies and procedures set by Visma Group. Within 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 e-conomic. Managers are responsible for the daily information security compliance and contribute towards the achievement of e-conomic's operational information security processes and procedures.

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

3.7 Human resources security (A.7)

3.7.1 Screening

Prior to employment, 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 e-conomic's main assets is the employees, and 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 onboarding sessions, where employees receive an introduction to internal policies related to data protection as well as a walkthrough of our information security policies.

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

3.8 Access control (A.9)

3.8.1 Access Control Policy

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 can only be done with privileged user rights, which are requested as time-based tokens and can only be performed by vetted personnel while producing an audit trail.

Requests for privileged users are done using the Visma MIMPortal, based on Microsoft Active Directory with the Microsoft Identity Manager (MIMPortal) as a frontend. Employees of e-conomic must request privileged user access using MIMPortal.

3.8.3 Review of user access rights

The team responsible for the production environment within the Product Unit of 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. Service owners are reviewed periodically to ensure that only authorised persons can accept access requests to the production environment. Privileged access is only granted as time-based tokens up to a maximum of 8 hours for specific roles.

Periodic reviews of access rights for systems that grant access to our code or application data without time-based access are performed on a regular basis. These systems include Sendgrid, MessageCloud by SmartFocus, CloudAMQP and Datadog. The periodic reviews are conducted by the owner of each system.

3.8.4 Removal or adjustment of access rights

Upon termination of employment, 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 e-conomic. For any systems not controlled centrally, 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 privileged accounts, employees are automatically enrolled in 2-factor authentication.

For our customer-facing e-conomic application, we require the use of signing up to Visma Connect, which is a Visma-provided login solution. Visma Connect requires the following password requirements in alignment with security standards:

- 8-character minimum
- 1 required digit (0-9)
- 1 required uppercase (A-Z) character
- 1 required lowercase (a-z) character
- 1 required special character.

In addition, our customers are also provided with the option to implement 2FA through Visma Connect.

3.8.6 Password management system

Visma's Active Directory enforces an industrial standard for length and complexity of the password.

Additionally, e-conomic uses 1Password as our password management system to enforce strong master passwords and multi-factor authentication when accessing production secrets. Access changes within the password management system are always logged.

3.9 Operations security (A.12)

3.9.1 Documented operating procedures

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, 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 Jira. 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 in Datadog, 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 and stored in Datadog. 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 e-conomic employees with work-related need access.

3.9.8 Installation of software on operational systems

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

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 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

When making changes to our source code, we use GitHub. GitHub is utilised by developers/engineers to make changes to source code development repositories. Access to GitHub is authorised and restricted to relevant employees.

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 applied in GitHub.

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

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
- 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.

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 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

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 e-conomic responded, document the root cause, and make note of preventative actions to be taken.

3.13.2 Reporting information security events

All e-conomic employees are responsible for reporting potential incidents to the security 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

The e-conomic application 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 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 e-conomic's customers with information about the controls at e-conomic that may affect the processing of user organisations' account data and also to provide e-conomic's customers with information about the operating effectiveness 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 e-conomic.

Our testing of 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, e-conomic's controls may not compensate for such weaknesses.

Our examination included corroborative inquiry of the appropriate management, supervisory, and staff personnel, inspection of documents and records, observation of activities and operations, and re-performance of tests of controls performed by e-conomic. Our tests of controls were performed on controls as they existed for the period from 1 January 2023 to 31 December 2023 and were applied to those controls specified by e-conomic.

The descriptions of controls are the responsibility of e-conomic's management. Our responsibility is to express an opinion about whether:

1. The description presents fairly, in all material respects, the aspects of e-conomic's controls that may be relevant to a user organisation's internal control;
2. The controls included in the description were suitably designed and implemented to meet the applicable control stated in management's description; and
3. The controls included in the description were operating effectively to meet the applicable control.

4.2 Description of Testing Procedures Performed

Our examination included inquiry of management, supervisory, and staff personnel; inspection of documents and records; observation of activities and operations; and reperformance of controls surrounding and provided by e-conomic. Our tests of controls were performed on controls as they existed throughout the period from 1 January 2023 to 31 December 2023.

The tests performed of the operating effectiveness of controls are described below:

Method	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the reporting period and is accompanied by other procedures stated below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed performance of the control multiple times throughout the reporting period to evidence application of the specific control activity.
Examination of documentation/ Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperformed the procedures. Compared any exception items identified with those identified by the responsible control owner.

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 2023 to 31 December 2023.

Our test of the operating effectiveness of controls was designed to cover a representative number of transactions throughout the period from 1 January 2023 to 31 December 2023 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 Reporting on Results of Testing

The results of the testing of the control environment and controls were sufficient to conclude that controls were operating effectively to provide reasonable, but not absolute, assurance that the applicable controls were achieved for the period from 1 January 2023 to 31 December 2023.

It is each interested party’s responsibility to evaluate this information in relation to internal controls in place at each user organisation to assess the total system of internal control. If it is concluded that the user organisation does not have effective internal controls in place, e-conomic’s internal controls may not compensate for such weaknesses.

4.5 Control objectives, controls, and test results

4.5.1 Information Security Policy (A.5)

Control Area	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.5.0.1 *Policies for risk security*	A set of policies for Risk Assessment shall be defined, approved by management, published and communicated to employees and relevant external parties.	Inquired of relevant personnel to understand whether the Risk Assessment is defined, approved by management, published and communicated to employees and relevant external parties. Inspected the policies for risk assessment to ascertain that they were reassuringly designed and approved by management. Inspected documentation of Visma's intranet to ascertain that the risk assessment policy is published.	No exceptions noted.
A.5.1.1 *Policies for information security*	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 in e-conomic.	Inquired of relevant personnel to understand whether a management-approved IT security policy has been published and communicated to relevant employees in e-conomic. Inspected the IT security policy to ascertain whether it was reassuringly designed and approved by management. Inspected documentation of Visma's intranet to ascertain whether the IT security policy is published. Inspected documentation of Visma's onboarding training to ascertain that the IT security policy is communicated to relevant employees.	No exceptions noted.
A.5.1.2 *Risk assessment*	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.	Inquired of relevant personnel to understand whether e-conomic has a management-approved risk assessment documenting main risks to the business and service offered. Inspected documentation of the risk assessment to ascertain whether it covers risks to the business and service offered.	No exceptions noted.

Control Area	e-conomic's control activity	Test performed by Deloitte	Test Results
		Inspected documentation to ascertain whether the risk assessment is approved and reviewed in the audit period.	
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.	Inquired of relevant personnel to understand whether the IT security policy is evaluated annually or upon significant changes. Inspected documentation of management's review of the IT security policy to ascertain whether it was evaluated in the audit period.	No exceptions noted.

4.5.2 Organisation of Information Security (A.6)

Control Area	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	e-conomic has allocated roles and responsibilities as stated in the Information Security Policy, and the employees are familiar with their tasks and responsibilities to ensure proper handling of security-related activities.	Inquired of relevant personnel to understand whether roles and responsibilities have been allocated, and employees are aware of their tasks. Inspected the IT security policy to ascertain whether roles and responsibilities have been allocated. For a sample of employees, inquired of their roles and responsibilities to ascertain whether they could demonstrate sufficient knowledge of their roles and responsibilities.	No exceptions noted.

4.5.3 Human resource security (A.7)

Control Area	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	e-conomic screens 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 the production SQL server, 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.	Inquired of relevant personnel to understand the process for screening job applicants to ensure suitable candidates. For a sample of new hires, inspected documentation to ascertain that: • A Reference Check was conducted • Contracts include a non-disclosure agreement For a sample of new hires that have been granted access to the SQL server, inspected documentation to ascertain whether a criminal record is obtained prior to the recruitment of the candidate.	No exceptions noted.
A.7.2.2 Information security awareness, education and training	e-conomic conducts training related to information security through onboarding sessions with new employees as well as periodic e-learning courses.	Inquired of relevant personnel to understand the process for conducting information security training of new employees along with periodic e-learning courses. Inspected the training material used for training of new employees to ascertain that this includes information security training. For a sample of new employees, inspected documentation to ascertain that the mandatory training was completed within the audit period.	No exceptions noted.

4.5.4 Access control (A.9)

Control Area	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.	Inquired of relevant personnel to understand whether an access control policy has been established, documented and reviewed. Inspected the access control policy to ascertain whether it has been established, documented and reviewed.	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.	Inquired of relevant personnel to understand the process for allocating access rights based on position and department. For a sample of granted access rights, inspected documentation to ascertain whether they were based on position and department.	No exceptions noted.
A.9.2.3 – Management of privileged 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.	Inquired of relevant personnel to understand the process of granting time-based access to customer data and systems. Inspected the procedures for granting access to the production environment to ascertain whether privileged access is granted on a time-based basis and must be approved by the service owner. For a sample of granted privileged access inspected documentation to ascertain whether: • Access privileges are authorised and appropriate for the user's assigned duties based on business justification and approval from the service owner. • Access privileges are given on a time-based basis.	No exceptions noted.
A.9.2.5 – Periodic Review of access rights	Periodic reviews of access rights for systems that grant access to our code or application data without time-based access are performed on a regular basis by the system owner.	Inquired of relevant personnel to understand the process for periodic reviews of access rights. For a sample of user access review, inspected documentation to ascertain whether: • Review was properly documented and performed at the appropriate level of detail. • Review had been performed by the owner of the system.	No exceptions noted.

Control Area	e-conomic's control activity	Test performed by Deloitte	Test Results
A.9.2.6 *Removal or adjustment of access rights*	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.	Inquired of relevant personnel to understand the procedure for closing user accounts or disabling users. For a sample of terminated employees, inspected documentation to ascertain whether their user accounts had been disabled in the internal directory.	No exceptions noted.
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's information security policy. Passwords are configured as follows. ● Password length regular user: 15 characters ● Password length service account: 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.	Inquired of relevant personnel to understand the password policy that has been established. Inspected the password policy to ascertain that it includes requirements for relevant password settings. Inspected the password settings that are configured for Google Cloud Platform, GitHub, e-conomic application, 1Password and Microsoft Identity Manager to ascertain whether passwords have been configured in alignment with policies.	No exceptions noted.
A.9.4.3 *Password management system*	Production secrets are stored in a password management system using encryption, and never stored in clear text. Access to the password management system is limited to employees with a work-related need.	Inquired of relevant personnel to understand the process of storing and access of production secrets in the password management tool '1Password'. Inspected documentation from 1Password to ascertain whether encryption is enabled. Inspected documentation from 1Password to ascertain whether employees with access have a work-related need.	No exceptions noted.

4.5.5 Operations security (A.12)

Control Area	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	e-conomic has written guidelines and procedures for operations, development and maintenance of systems.	Inquired of relevant personnel to understand whether written guidelines for operation, development and maintenance of systems are in place. Inspected documentation of the written guidelines to ascertain whether they include procedures for operations, development and maintenance of systems.	No exceptions noted.
A.12.1.2 Change management	e-conomic has defined change management procedures regarding secure development, test and deployment processes.	Inquired of relevant personnel to understand whether a definition of the change management procedures has been established. Inspected the procedures for change management to ascertain whether they cover considerations on secure development, test and deployment processes. For a sample of deployed changes, inspected documentation to ascertain whether they were tested, reviewed and approved prior to implementation.	No exceptions noted.
A.12.1.3 Capacity management	e-conomic has implemented a process for capacity management, which is supported by various tools to monitor capacity and operational errors. e-conomic has established a status page in e-conomic showing historical and current operational incidents.	Inquired of relevant personnel to understand the process and tools used for monitoring and adjustment of capacity to ensure availability. Inspected documentation of the e-conomic status page to ascertain that it includes historical and current operational incidents.	No exceptions noted.
A.12.1.4 Separation of development, testing and operational environments	e-conomic has separated development, test and production environments on different servers.	Inquired of relevant personnel to understand whether environments have been separated on different servers. Inspected documentation from Google Cloud Platform to ascertain whether separation of development, testing and operating environments is established on different servers.	No exceptions noted.
Control objective: To protect against loss of data.			
A.12.3.1 Information backup	e-conomic has established backup procedures for e-conomic.	Inquired of relevant personnel to understand the process of backup and restore for e-conomic.	No exceptions noted.

Control Area	e-conomic's control activity	Test performed by Deloitte	Test Results
	Restoration of data from backup systems is tested regularly. Backups are stored in two geographically redundant environments.	Inspected documentation to ascertain whether a backup strategy for e-conomic has been established and is complied with. For a sample of restore tests, inspected documentation to ascertain whether restore of backup has been performed on a weekly basis. For a sample of backups, inspected documentation to ascertain that backups are stored in two geographically redundant environments.	
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.	Inquired of relevant personnel to understand whether the process of event logging has been enabled. Inspected documentation to ascertain whether event logging of user activity, exceptions and errors have been enabled and a retention period have been configured.	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 restricted with view access.	Inquired of relevant personnel to understand the process in place for safeguarding logs. Inspected documentation to ascertain whether relevant logs are stored. Inspected documentation to ascertain whether access to the logs is restricted with view access.	No exceptions noted.

Control Area	e-conomic's control activity	Test performed by Deloitte	Test Results
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.	Inquired of relevant personnel to understand the patch management process. Inspected documentation of the build of the base application image configuration to ascertain whether it is performed weekly and with the most recent images available with the cloud provider. Inspected documentation of the latest database servers to ascertain whether they have been patched with the latest patch.	No exceptions noted.
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.	Inquired of relevant personnel to understand the process for monitoring and handling of technical vulnerabilities for e-conomic. For a sample of technical vulnerabilities, inspected documentation to ascertain whether they have been evaluated on a timely basis, and appropriate measures have been taken to address the associated risks.	No exceptions noted.

4.5.6 Communications security (A.13)

Control Area	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*	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.	Inquired of relevant personnel to understand whether the network has been secured to avoid unauthorised access and protect information in e-conomic. Inspected documentation to ascertain whether access to the network is restricted by access controls and separation of network services. Inspected documentation of the firewall rules implemented in e-conomic to ascertain whether they are configured appropriately. For a sample of changes to the network infrastructure, inspected documentation to ascertain whether they have been peer-reviewed 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. e-conomic has segregated the network into subnets covering internal-, staging-, sandbox- and production environments.	Inquired of relevant personnel to understand the process of segregating the network. Inspected the password configuration to the wireless network to ascertain whether access requires a valid username and password. Inspected documentation of the network segregation in subnets to ascertain whether, they are segregated into internal, staging, sandbox and production environments.	No exceptions noted.

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

Control Area	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*	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.	Inquired of relevant personnel to understand the system change control procedure. Inspected documentation of the system change control procedure to ascertain whether it is supported by workflows. For a sample of changes, inspected documentation to ascertain whether they were supported by workflows from the change management system ensuring that each step had been documented.	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.	For a sample of changes, obtained and inspected documentation to ascertain that they were tested prior to implementation.	No exceptions noted.
A.14.2.8 *System security testing*	e-conomic has established procedures for securing functionality testing during development for e-conomic.	Inquired of relevant personnel to understand the procedures for securing functionality testing during the development stage. Inspected documentation to ascertain whether procedures have been established for securing functionality testing during the development stage. For a sample of changes, inspected documentation to ascertain that functionality testing was performed during development.	No exceptions noted.

4.5.8 Supplier service delivery management (A.15)

Control Area	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	e-conomic has established a process to monitor and review supplier services. e-conomic is monitoring and reviewing supplier services delivery on a regular basis.	Inquired of relevant personnel to understand the process of monitoring supplier services. Inspected documentation to ascertain whether e-conomic has procedures to monitor and review supplier services. For a selected sample of e-conomic suppliers, inspected documentation to ascertain whether monitoring and periodic review are performed.	No exceptions noted.

4.5.9 Information security incident management (A.16)

Control Area	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	e-conomic has established a procedure in which managerial responsibilities for management of information security breaches are determined.	Inquired of relevant personnel to understand whether procedures related to managerial responsibilities regarding security breaches have been determined. Inspected documentation to ascertain whether managerial responsibilities for management of information security breaches are determined.	No exceptions noted.
A.16.1.2 Reporting information security events	e-conomic has established a procedure to ensure that information security incidents are reported without undue delay.	Inquired of relevant personnel to understand the process of reporting information security incidents. For a sample of information security incidents, ascertained whether they were reported without undue delay.	No exceptions noted.
A.16.1.5 Response to information security incidents	e-conomic has established a procedure to ensure that information security incidents are reported in accordance with the documented procedures.	Inquired of relevant personnel to understand the process of reporting security incidents. For a sample of security incidents, obtained and inspected the IT Service Management system ticket to ascertain that: • The incident includes preventative actions to be taken. • The incident was communicated to customers when necessary. • The incident was resolved in a timely manner. • Root-cause analysis was performed.	No exceptions noted.