AUGUST 2018

UNICONTA A/S

ISAE 3402 TYPE 1 ASSURANCE REPORT

Independent auditor's report on coverage of the technical and organizational measures related to the operation of Uniconta A/S' cloud-based ERP system.

In addition, a control description has been provided with selected requirements from the General Data Protection Regulation and Uniconta A/S' role as a data processor.

Beierholm
Statsautoriseret Revisionspartnerselskab
Knud Højgaards Vej 9
2860 Søborg
CVR-nr. 32 89 54 68
Tlf +45 39 16 76 00

www.beierholm.dk

BEIERHOLM
VI SKABER BALANCE

Structure of the Assurance Report

Chapter 1:

Letter of Representation.

Chapter 2:

Description of the technical and organizational measures for the operation of cloud-based ERP system.

Chapter 3:

Independent Auditor's Assurance Report on the description of the technical and organizational measures, their design and their design.

CHAPTER 1:

Letter of Representation

This description in Chapter 2 incl. Appendix 1 of Uniconta A/S' technical and organizational measures has been prepared for customers, who have used or plan to use the Uniconta cloud-based ERP system, and their auditors, who have sufficient understanding to consider the description, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements. Uniconta A/S hereby confirms that

(A) The description in Chapter 2 incl. Appendix 1 gives a true and fair description of Uniconta A/S' technical and organizational measures in relation to the Uniconta cloud-based ERP system as at 31 August 2018. The criteria for this assertion are that this description:

(i) gives an account of how the controls were designed and implemented, including:

- the types of services delivered, when relevant
- the processes in both IT and manual systems that are used to manage the technical and organizational measures
- relevant control objectives and control procedures designed to achieve these goals
- control procedures that we have assumed – with reference to the system's design – would be implemented by the user companies and which, if necessary to fulfil the control objectives mentioned in the description, have been identified in the description together with the specific control objectives that we cannot fulfil ourselves
- other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that have been relevant for the technical and organizational measures

(ii) does not omit or misrepresent information that is relevant for the scope of the controls described, taking into consideration that the description has been 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 their own particular environment.

(B) The controls related to the control objectives stated in the accompanying description were suitably designed as at 31 August 2018. The criteria for this assertion are that:

(i) the risks that threatened the fulfilment of the control objectives mentioned in the description were identified

(ii) the identified controls would, if used as described, provide reasonable assurance that the risks in question would not prevent the fulfilment of these control objectives.

(C) The accompanying description and the related criteria for fulfilling the control objectives and controls, Chapter 2 incl. Appendix 1, have been prepared based on compliance with Uniconta A/S' standard agreement. The criteria for this basis are:

(i) Uniconta – Data Processing Agreement

(ii) Uniconta - Information Security Manual Version 1.0 as at 14-05-2018

Ballerup, 1 September 2018

Erik Damgaard, CEO & Founder **Claus Klein-Ipsen, CFO & Director**

Uniconta A/S, Klausdalsbrovej 601, 2750 Ballerup, Cvr. nr. 33266928

CHAPTER 2:

Description of the technical and organizational measures for the Operation of the Uniconta cloud-based ERP system

Introduction

The purpose of the current description is to offer information to Uniconta A/S' customers and their auditors concerning the relevant ISO 27002:2013 requirements and controls implemented in Uniconta A/S' security policy. ISO 27002:2013 is an information security standard published by the International Organization for Standardization (ISO).

The purpose of this description is exposure of the technical and organizational measures implemented in connection with the development and operation of the Uniconta cloud-based ERP system. As a supplement to the description, is added an independent paragraph (Compliance with the role as data processor), including a description of essential requirements regarding the role as data processor.

Furthermore, the description provides information about the controls applied for the operation of Uniconta A/S' cloud-based ERP system as of 31 August 2018.

Description of Uniconta A/S

Uniconta is a supplier of ERP software to businesses, organisations and accounting companies. The core activity in Uniconta is the development and operation of the cloud-based ERP system.

The solution is supplied as a service hosted in data centers operated by Uniconta A/S' hosting providers.

Scope of this description

As a SaaS supplier, Uniconta is responsible for establishing and maintaining relevant procedures and controls regarding the development and operation of the Uniconta cloud-based ERP system, ensuring that any security issue is identified and managed according to the requirements laid down in the agreements with the customers.

This description is based on Uniconta's security policies governing the everyday operations of the Uniconta cloud-based ERP system, and the relevant parts of Uniconta's Data Processing Agreement with its customers.

Business strategy / IT security strategy

Uniconta software is designed to be secure, so that neither the customers nor the company is subjected to any unacceptable security risks.

The purpose of Uniconta's IT security strategy is to ensure:

- The existence of relevant prerequisites for secure operations of the Uniconta cloud-based ERP system
- Uniconta software and customer data are sufficiently protected against incidents
- Systems and data can be reestablished with predictability and according to familiar working methods
- Customer data is accessed by relevant Uniconta personnel, when carrying out necessary tasks
- That exclusively authorized persons have access to the operating environment, systems and data

Uniconta works with IT security at a business-strategic level to ensure a high degree of service and quality. The IT security policy emphasizes the importance of IT security in the company. In relation to its IT security strategy, Uniconta has chosen to take ISO 27002:2013 as its starting point, and has used the ISO method to implement the relevant security measures within the following areas:

- Information security policies
- Organisation of information security
- Human resources security
- Asset management
- Access control
- Physical and environmental security
  Operations security
- Communications security
- System acquisition, development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

In addition, Uniconta's Data Processing Agreement (DPA) binds the company to implement relevant security measures regarding:

- Data processing activities conducted on behalf of the customers (item 3 and 7 in the DPA)
- Data breach monitoring and reporting (item 6 in the DPA)

The implemented security measures at Uniconta are described in appendix 1.

Uniconta A/S' organization and organization of IT security

Uniconta employs approximately 20 employees and has a flat organizational structure. The CEO manages the company together with the senior management group.

In order to ensure the correct level of focus on information security, Uniconta has appointed a specific Information Security Committee acting on behalf of the management and taking the responsibility of security issues. In 2018, the board consisted of:

- Claus Klein-Ipsen, CFO
- Jørn Rejndrup, Executive vice president and head of Support and Sales

Risk management at Uniconta A/S

The purpose of the information security policy is to define a framework for the protection of valuable information and, in particular, to ensure that critical and sensitive information and information systems maintain their confidentiality, integrity and accessibility.

Therefore, Uniconta's management has chosen a risk-based information security management system, ensuring that all notable threats are mitigated in an appropriate manner. This way, predictable security problems can be prevented and potential damage limited, ensuring effective restoration of information in case of an incident.

The risk management policy is established to cover or limit the risks created by everyday activities to a level enabling the company to maintain normal operations. Uniconta carries out risk management and internal checks in relevant areas and levels: the risk and impact assessment process is executed annually, in order to keep the management aware of the risk profile of Uniconta. Risk assessments are also conducted, if significant changes take place in the company.

Uniconta has carried out a risk analysis and drawn up the Uniconta Information Security Management System based on the results of the risk assessment. Furthermore, an incident response policy with a corresponding disaster recovery plan has been created utilizing the outcome of the risk management process.

Uniconta also works with the known international standards for IT security. The ISO 27002:2013 is the primary reference framework for IT security used at Uniconta. The work process regarding IT security is a continual and dynamic process, ensuring that Uniconta at all times complies with its customers' needs, and with legal and contractual requirements.

IT security execution

The management of Uniconta has the day-to-day responsibility for IT security, ensuring that the overall requirements and framework for IT security are maintained. To ensure that information security is appropriately addressed at Uniconta, the management has appointed an Information Security Board to handle security related work in Uniconta. The Information Security Board always consists of the Chief Financial Officer and a minimum of one other member of the senior management group.

The structure of the Uniconta ISMS is described in the central IT security policy prepared by the management. The aim of the Uniconta ISMS is to provide the company with a shared set of rules and guidelines regarding information security, ensuring a stable and secure operating environment. Uniconta makes regular improvements to policies, procedures and operations to ensure that both our customers' requirements and relevant legislation are complied with.

Uniconta’s IT security focus is on everyday development and operations, and the ability to ensure that a well-functioning Uniconta offers services to the customers at an acceptable level. The ISMS applies to all employees without exception, both permanent and temporary staff, and, where relevant, to outsourced workforce working for Uniconta.

When outsourcing parts of Uniconta’s development or operations, the service provider must cooperate with Uniconta to ensure the appropriate security level as well as ensuring operations being executed in accordance with the Uniconta ISMS. Uniconta protects its information and solely allows use of and access to information in accordance with the company's guidelines and current legislation.

HR, employees and training

Uniconta acknowledges the fact, that its employees play an important role in the information security of the company. Uniconta has therefore implemented measures to ensure appropriate processes concerning information security prior to, during and after employment. The CFO and direct line managers have specified responsibilities to perform the relevant tasks set out in the specific guidelines.

All individuals employed by Uniconta are subject to screening prior to employment. The screening is in accordance with the defined process.

Employees are furthermore contractually informed and obliged to follow the rules and guidelines set out by the management of Uniconta regarding information security.

During the employment at Uniconta, individual employees are obligated to participate in the information security awareness-training program covering both GDPR and general information security topics.

And in the case of termination of employment, Uniconta has a defined procedure to ensure that the relevant IT equipment is returned, and user access rights are closed or dealt with in other ways.

Asset management

Uniconta only owns a limited number of physical assets. Operating servers and IT infrastructure are primarily provided by trusted suppliers. Uniconta has an interest in ensuring that all assets are securely operated. Uniconta has therefore assigned ownership of each asset to specific employees within Uniconta.

Ownership of an assets means that the specified employee has the responsibility of ensuring that the asset is implemented and operated with respect to the overall objectives for the information security of Uniconta.

Ownership of assets can be delegated from the management to relevant employees.

Ownership of hardware and software assets is documented, reviewed and adjusted as part of the yearly risk assessment process.

Access control

Physical and logical access control is a high priority in Uniconta. There is a clear motivation to control access to Uniconta's assets and limit it to the people, who have a clear need-to-know and have tasks related to the access given.

Uniconta's overall guidelines to controlling the access to assets are documented in the access control policy.

Access control is focused on 1) access to the Uniconta IT-infrastructure and 2) access within the Uniconta cloud-based ERP system:

1) IT-infrastructure: Uniconta is dependent on suppliers for the IT-infrastructure and sets demands for the suppliers in terms of access management access management and user rights.

2) Within the Uniconta-Application: For cloud-based ERP system, a logical layered access control scheme is implemented, which ensures that the relevant user categories (both internal and external) have the appropriate access within the Uniconta system and underlying data.

Access control related to Uniconta's own network is defined in the Network Access Control Policy.

Physical and environmental security

Uniconta's offices are in a shared office space at the premises of the Danish insurance company, Tryg, in Copenhagen, Denmark. This means that there are high standards for the physical security and access to the offices. All employees have personal id-cards, which must be used for access. All visitors are registered in the reception area and there are physical barriers preventing unauthorized access to the building and office areas.

The IT infrastructure (servers) from where the Uniconta application is being operated is physically located in a datacenter in Denmark. Uniconta has entered into an agreement with the company, Hostingkompagniet, who is responsible for the physical security of the servers.

Employees are instructed to follow guidelines related to the daily work routines.

Operations security

In order to ensure an appropriate level of operational security, Uniconta has applied a variety of controls addressing security issues, covering:

- Firewall
- Backup and recovery
- Patch management
- Malware protection
- Monitoring
- Log management/SIEM
- Technical vulnerabilities management
- Separation of development, testing, and operation environments

The overview below will cover the parts of the policies considered relevant for external stakeholders.

Separation of development, testing, and operation environments
Uniconta has separate environments for development, test and production. The purpose of separate development, test and production environments is to ensure a continuous development of the cloud-based ERP system, while making sure that only changes which have been appropriately tested are launched into the production environment.

Backup and recovery
The backup policy ensures appropriate protection against loss of data and ensures the ability to restore production data that has been lost or corrupted in the client's system.
Backup copies of information, software and system images are taken and tested regularly in accordance with Uniconta's backup setup rules.

Logging and monitoring
Uniconta A/S logs system events and selected applications locally using a central logging solution. The logging facilities and log information are protected against tampering and unauthorized access.

Management of technical vulnerabilities
Uniconta Operations conduct continuous testing in order to identify technical vulnerabilities of information systems being used in Uniconta. In case of severe vulnerabilities being found, the exposure to such vulnerabilities is evaluated and appropriate measures are taken to reduce the risks to everyday operations.

Communications security

Uniconta uses primarily two networks, one for the office space and one for servers.

Uniconta's use of office network is limited to workstations and shared office resources, such as printers. The employees' use of the network is regulated by rules laid down in the IT-usage guidelines. Access to the network requires the assignment of connection right to the network, where access is assigned per user. This minimizes the risk of unauthorized access to the network.

The server network is operated by Hostingkompagniet and is strictly used for connection of the Uniconta servers only. This means that several security measures are implemented on the network.

Networks are in this way segregated by default: One network for employees and workstations and another network for the UC-application.

System acquisition, development and maintenance

The development of the Uniconta cloud-based ERP system is one of the primary activities of Uniconta. The quality and stability of the ERP system has a direct influence on the overall company.

Therefore, there is a strong focus on securing that the development of the ERP system meets the requirements of Uniconta's customers and partners.

Uniconta has established separate environments for the development, test and production of the cloud-based ERP system.

The overall goal is to ensure that updates and new developments meet high standards by monitoring development, testing and approving processes before release and at the same time maintain a flexible approach, which enables Uniconta to constantly develop the ERP system.

Uniconta has established guidelines and processes for the development and release of updates.

These guidelines include:

1) Defined responsibilities
2) Guidelines for development
3) Categorization of bugs and developments task
4) Development process
5) Testing process
6) Release process

Supplier relationships

Uniconta works with suppliers in operating and developing the Uniconta cloud-based ERP system. For key suppliers, who have access to customer instances, it is mandatory to have GDPR-compliant sub-processing agreements in place with Uniconta, compelling the suppliers to follow the same regulations as Uniconta. Relevant suppliers must also be compliant with Uniconta's information security policies.

Uniconta is dependent on a few key suppliers in its daily operation and development of the Uniconta cloud-based ERP system.

See below for a short description of Uniconta' main type of suppliers regarding the development and production of the Uniconta software application:

1) Outsourcing partners for development resources – Uniconta recruits and facilitates IT development resources through key suppliers
2) Hosting provider – Responsible for the operation and support related to the IT infrastructure of Uniconta (servers).
3) TRYG – responsible for operating the physical office space and network access in the office.

All supplier relationships are governed through formal agreements.

To ensure that information security is evaluated and prioritized before entering into agreements with new suppliers, Uniconta has defined specific policies for selection of suppliers.

Agreements with key suppliers are reviewed annually.

Managing IT security incidents

Uniconta incident management policies are devised to ensure quick detection, reaction and response to security incidents, and to outline the processes followed after a security incident.

All employees at Uniconta are familiar with the procedures for reporting different types of incidents and weaknesses, which can influence operational security. Security incidents and weaknesses must be reported as quickly as possible to the management group.

The management group is responsible for defining and coordinating a structured management process that ensures an appropriate reaction to security incidents. All Uniconta's employees, partners, contractors and suppliers have a responsibility to report security incidents and data breaches as quickly as possible to Uniconta's CFO. This obligation also extends to any external organisation contracted to support or access the Uniconta Information Systems.

Uniconta is responsible for the security and integrity of all the data, it keeps. Uniconta protects data using all means necessary: incidents affecting data security are prevented and/or minimized in the best way possible. In case of an identified data breach, Uniconta follows a specific data breach handling process.

All critical incidents are handled according to Uniconta's incident handling process, and an incident report is produced and shared with the customer affected by the incident. Reporting critical incidents causes relevant Uniconta employees and managers to be alerted to ensure efficient incident handling.

Review of the event will be undertaken by the CFO together with relevant employees and managers to establish the cause of the incident, the efficiency of the response and to identify areas that require improvements. Lastly, recommended changes to systems, policies and procedures are documented and implemented as soon as possible.

Information security aspects of business continuity management

Uniconta has a business continuity plan, which defines the actions needed to be taken in the case of security incidents that are affecting the Uniconta application.

Measures have been implemented to ensure that the production environment is protected and that relevant redundancies are in place and that service can be restored in case of hardware and/or software failures.

Compliance with the role as Data Processor

It is the responsibility of Uniconta A/S' management to ensure that all relevant legal and contractual requirements are identified and complied with correctly. Relevant requirements might be, e.g:

- The EU General Data Protection Regulation
- The Danish Data Protection Act
- Data Processor Agreements
- Uniconta ApS standard contract or other relevant sources

The existence of all necessary agreements, a comprehensive ISMS (management system for managing information security) as well as other relevant documents, ensure compliance with all relevant legal and contractual requirements.

Uniconta A/S is obliged to involve legal experts as needed to ensure compliance with law and regulations.

Furthermore, Uniconta A/S' senior management reviews all Uniconta A/S' security policies on a regular basis, including involving any relevant stakeholders. Uniconta A/S' ISMS is regularly audited by an independent, external party, and on request the audit report is shared with all Uniconta A/S' customers.

The EU General Data Protection Regulations (GDPR)
Uniconta cloud-based ERP system enables our customers to collect, process and report on data they collect from respondents or other data inputs. Uniconta does not own the data our customers collect, but develops and operates the software for our customers to utilise.

According to the EU General Data Protection Regulations and Danish additional regulation (The Danish Data Protection Act), Uniconta A/S is the Data Processor, and the customer is the Data Controller.

Uniconta A/S cooperates with legal experts to ensure that all legal requirements are identified and accommodated. Uniconta A/S has also ensured relevant contracts with all key stakeholders (including customers, business partners, key suppliers etc.) to ensure compliance with law and regulations. In addition, Uniconta A/S works together with the customers to ensure that the customers are aware of and comply with the relevant GDPR rules.

According to GDPR, compliance with the ISO 27002:2013 standard ensures an appropriate security level. Besides compliance with the relevant ISO requirements, Uniconta A/S ensures data privacy and data security on a contractual level.

Privacy and protection of personal data

As mentioned above, Uniconta A/S is the customers' Data Processor, given that the customers are offered an IT service to which they can to transfer and process data, and utilize it for further processing within their respective administrative assignments. Uniconta A/S is not responsible for any data uploaded by the customers to their Uniconta IT service. Based on the categories and confidentiality of the data entrusted to Uniconta A/S by the customers, Uniconta A/S must put all necessary security measures required into practice to ensure an appropriate level of security.

Below is described Uniconta A/S' procedures of how Uniconta A/S operates as Data Processor according to directions from the Data Controllers.

Data Protection Agreements

Uniconta has Data Processor Agreements (DPA) in place with all of our customers. These contracts outline Uniconta's role and responsibilities as Data Processor, and the customer's role and responsibilities as Data Controller.

According to our standard DPA, Uniconta keeps a record of processing activities carried out on behalf of our customers. The records include:

- The name and contact information of the supplier, the sub-processors, and the customer.
- The categories of processing carried out by the supplier or any sub-processors on behalf of the customer.
- Transfer of personal data, if any, outside of EEA, including the name of any sub-processor and the concerned country or countries outside of EEA.
- Where possible, a general description of the technical and organisational security measures undertaken by the supplier to safeguard the personal data.

At the request of the customer, Uniconta A/S must make the processing activities list available to the customer or to the Danish Data Protection Agency (Datatilsynet) at any time.

Access to the data in customer instances

In general, Uniconta A/S does not access any customer instances unless specifically appointed by the customer.

In short, Uniconta A/S does not access the data collected by its customers, unless specifically asked by the customer. Only specific employees at Uniconta A/S are allowed to access customers' data upon request.

Important changes in relation to IT security

Uniconta's IT-security strategy, the relevant framework and the ISMS have undergone a large-scale change during 2018 as a part of our security focus. The implementation of the latest version has caused the establishment of a wide variety of new security controls during the process. Uniconta's aim has been that all the security controls presented above were implemented by the 24th of May 2018.

Uniconta A/S will continue to work with information security in 2018 with focus on the relevant legislation, further improving the current controls and improving security controls around software development practices. We are committed to a new audit by an external auditor in a year, and will share the audit report, when it has been made available to us.

Customers' responsibilities (complementary controls at the customer)

The above description is based on the Uniconta ISMS and other standard contractual clauses. This means that no account has been made for the agreements of individual customers.

Uniconta expects the customer to handle the access control to the customer’s own instance. Uniconta grants the access to an appointed person working for the customer during onboarding, and afterwards it is the customer’s responsibility to ensure that the access rights to their instance are appropriately controlled. The customer must have relevant access control restrictions in place in order to ensure the security of their Uniconta instance.

The responsibility for the daily use of Uniconta's platforms and customizations herein lies with the customer. Uniconta A/S is not responsible for the customer’s use of the software; it is the customer's own responsibility to ensure that the necessary internal security controls are in place, when using the Uniconta cloud-based ERP system. In general, Uniconta recommends risk-based evaluations to take place when planning any changes to a Uniconta instance: as the customer has the option to modify their instance, the potential risks created by the modifications should always be assessed and limited.

Furthermore, Uniconta does not take the responsibility regarding the data a customer collects and processes using their Uniconta instance. As described above, Uniconta does not access any customer instances, unless specifically asked by the customer, thus Uniconta does not know, what kind of data the customer is collecting.

APPENDIX 1:

Uniconta A/S applies the following control objectives and security measures from ISO27002:2013

5. Information Security Policies

5.1. Management directions for information security

6. Organisation of Information Security

6.1. Internal organisation
6.2. Mobile devices and teleworking

7. Human Resource Security

7.1. Prior to employment
7.2. During employment
7.3. Termination or change of employment

8. Asset Management

8.1. Responsibility for assets
8.3. Media handling

9. Access Control

9.1. Business requirements of access control
9.2. User access management
9.3. Users' responsibility

12. Operations Security

12.1. Operational procedures and responsibilities
12.2. Protection from malware
12.3. Backup
12.4. Logging and monitoring
12.5. Technical vulnerability management

13. Communications Security

13.1. Network security management
13.2. Information transfer

14.System acquisition, development and maintenance

14.1. Security requirements of information systems
14.2. Security in development and support processes
14.3. Test data

15. Supplier Relationships

15.1. Information security in supplier relationships
15.2. Supplier service delivery management

16. Information Security Incident Management

16.1. Management of information security incidents and improvements

17. Information Security Aspects of Business Continuity Management

17.1. Information security continuity
17.2. Redundancies

18. Compliance

18.1 Compliance with legal and contractual requirements

CHAPTER 2:

Independent Auditor's Assurance Report on the Description of the Technical and Organizational Measures and their Design

For the customers / users of Uniconta A/S' cloud-based ERP system and their auditors

Scope

We have been engaged to report on Uniconta A/S' description in Chapter 2 (incl. appendix 1) which is a description of technical and organizational measures conducted in connection with the Uniconta cloud-based ERP system as of 31 August 2018 and on the design of the controls mentioned in the description.

We have not conducted any procedures in relation to the operating functionality of the controls mentioned in the description, and thus express no opinion in this regard.

We express our opinion with reasonable assurance.

The report is based on a partial approach, which means that the present report does not include the IT security controls and control activities related to the use of external business partners. Uniconta A/S uses external partners in the following areas:

- Hosting activities and operational tasks from Hostingkompagniet A/S and Broadway 33 ApS. The solutions cover the following categories: SaaS (Software as a Service), PaaS (Platform as Service) and IaaS (Infrastructure as a Service).

The scope of our report does not cover customer-specific conditions, and the report does not include the complementary controls and control activities conducted by the user company; see the description of the company in Chapter 2 under the section: Complementary controls.

The current IT security strategy with accompanying framework and ISMS (IT security handbook) were devised and implemented during the period May to July 2018. The development of IT security has led to further control measures being devised and implemented during the implementation period.

It has been our underlying basis, that the complete IT security framework and accompanying IT security controls should be in effect from the middle of July 2018. All direct controls carried out once, twice or four times a year have, as far as it has been possible, been conducted within the said period and until 31 August 2018.

Uniconta A/S' responsibility

Uniconta A/S is responsible for the preparation of the description and accompanying assertions in Chapter 2 (incl. appendix 1), including the completeness, accuracy and method of presentation of the description and assertion; for providing Uniconta cloud-based ERP system as covered by the description; for stating the control objectives; and for designing, implementing and effectively operating controls to achieve the stated control objectives.

Beierholm's independence and quality management

We have complied with the requirements of independence and other ethical requirements laid down in FSR's Ethical Rules based on fundamental principles of integrity, objectivity, professional competence and requisite care, confidentiality and professional conduct.

We apply ISQC 1 and thus sustain a comprehensive system of quality management, including documented policies and procedures for compliance with ethical rules, professional standards as well as requirements in force under existing laws and additional regulation.

Auditor's responsibility

Our responsibility is to express an opinion on Uniconta A/S' description and on the design and implemented related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organisation, issued by the IAASB. The standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and whether the controls are appropriately designed in all material respects.

An assurance engagement to report on the description and design of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of the technical and organizational measures related to the Uniconta cloud-based ERP system as well as for the design of the controls.

The procedures selected depend on the judgement of the service organisation's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified and described in Chapter 2 (including appendix 1) by Uniconta A/S. As stated above, we have not conducted procedures related to the operating functionality of the controls included in the description, and thus we express no opinion in this regard.

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

Limitations of controls at Uniconta A/S

Uniconta A/S' description is prepared to meet the common needs of a broad range of customers and their auditors and thus may not include every aspect of the system that each individual customer may consider important in their own particular environment. In addition, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

Our opinion is based on the matters outlined in this report. The criteria on which our opinion is based are those described in Chapter 1 under Letter of Representation. In our opinion,

a) The description fairly presents the technical and organizational measures of Uniconta A/S for Uniconta cloud-based economy system, such as they were designed and implemented at 31 August 2018 in all material respects; and

b) The controls related to the control objectives stated in the description were in all material respects suitably designed at 31 August 2018.

Please, note that there may be specific circumstances in relation to the individual customers, which mean that the general conclusion is not fully adequate. If it has been agreed between the customer and Uniconta A/S that a specific statement should be prepared regarding the customer's contract, the conditions will appear from hereof.

Intended users and purpose

This report and the description are intended only for Uniconta A/S’ customers and their auditors, who have sufficient understanding to consider them, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatement in their financial statements.

Copenhagen, 1 September 2018

Beierholm
State Authorized Public Accountants

Kim Larsen	Jesper Aaskov Pedersen
State-authorized Public Accountant	IT-auditor, Manager