

JULY 2023

## CONTINIA SOFTWARE A/S

ISAE 3402 TYPE II ASSURANCE REPORT

CVR 32658083

Independent auditor's Report on the control environment in relation to the operation of Continia Online Services.

In addition, a paragraph has been added to the description about the role as data processor in accordance with the General Data Protection Regulation.

Beierholm  
State Authorized Public Accountants  
Copenhagen  
Knud Højgaards Vej 9  
DK-2860 Søborg  
Denmark  
CVR no. DK 32 89 54 68  
Tlf +45 39 16 76 00

[www.beierholm.dk](http://www.beierholm.dk)



# Structure of the Assurance Report

## Chapter 1:

Letter of Representation.

## Chapter 2:

Description of the control environment for the operation of Continia Online Services.

## Chapter 3:

Independent auditor's assurance report on the description of controls, their design and operating effectiveness.

## Chapter 4:

Auditor's description of control objectives, security measures, tests and findings.

# Letter of Representation

Continia Software A/S (hereafter referred to as "Continia") processes personal data on behalf of customers according to Data Processor Agreements regarding operation of Continia Online Services.

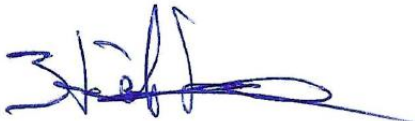
The accompanying description has been prepared for the use of customers and their auditors, who have used Continia Online Services, and who have sufficient understanding to consider the description along with other information, including information about controls operated by the customers i.e. the Data Controllers themselves, when assessing, whether the demands to the control environment as well as requirements laid down in the General Data Protection Regulation are complied with.

Continia hereby confirms that

- (A) The accompanying description, Chapter 2 (incl. Appendix 1) gives a true and fair description of Continia's control environment in relation to operations of Continia Online Services throughout the period 1 May 2022 – 30 April 2023. The criteria for this assertion are that the following description:
- (i) Gives an account of how the controls were designed and implemented, including:
    - The types of services delivered, including the type of personal data processed.
    - The processes in both IT and manual systems that are used to initiate, record, process and, if necessary, correct, erase, and limit the processing of personal data.
    - The processes are utilized to ensure that the performed data processing was conducted according to contract, directions or agreements with the customer i.e. the Data Controller.
    - The processes securing that the persons authorized to process personal data have pledged themselves to secrecy or are subject to relevant statutory confidentiality.
    - The processes securing that - at the Data Controller's discretion - all personal data is erased or returned to the Data Controller, when the data processing is finished, unless personal data must be stored according to law or regulation.
    - The processes supporting the Data Controller's ability to report to the Supervisory Authority as well as inform the Data Subjects in the event of personal security breaches.
    - The processes ensure appropriate technical and organizational security measures for processing personal data, taking into consideration the risks connected to processing, in particular accidental or illegal actions causing destruction, loss, change, unauthorized forwarding of or access to personal data that is transmitted, stored or in other ways processed.
  - (ii) Includes relevant information about changes in the operation of Continia Online Services performed throughout the period 1 May 2022 – 30 April 2023
  - (iii) Does not omit or misrepresent information 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 therefore not, include every aspect of the control 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 and operated effectively throughout the period 1 May 2022 – 30 April 2023. The criteria for this assertion are that:

- (i) The risks threatening the fulfillment 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 fulfillment of the said control objectives, and
  - (iii) The controls were applied consistently as designed, including that manual controls were performed by persons with adequate competencies and authority throughout the period 1 May 2022 – 30 April 2023.
- (C) Appropriate technical and organizational security measures are established in order to honor the agreements with the Data Controllers, generally accepted data processor standards, and relevant demands to Data Processors according to the General Data Processing Regulations.
- (D) 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 Continia's standard agreement as well as the related Data Processing Agreement. The criteria for this basis are:
- (i) Continia IT Security Strategy
  - (ii) Continia IT-Security Manual for Continia Online Services
  - (iii) Continia – Data Processor Agreement

Nørresundby, July 10th 2023



**Henrik Lærke, CEO**

Continia Software A/S, Stigsborgvej 60, DK-9400 Nørresundby, CVR 32658083

**Continia Software A/S**  
Stigsborgvej 60  
DK-9400 Nørresundby

Tlf. +45 8230 5000  
mail@continia.dk - www.continia.dk

CVR/VAT 3265 8083

# Description of control environment in connection with operation of Continia Online Services

## 2. The framework for control description

### 2.1 Introduction

The purpose of this description is to provide Continia Software A/S' customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organizations.

The scope of this description is to provide insights into the technical and organizational security measures implemented in connection with the operation of the Continia Online Services (COS).

As a supplement to the description below, an independent paragraph (accordance with the role as a data processor) is added, including a description of essential requirements regarding the role as data processor in combination with requirements laid down in our Data Processor Agreements.

### 2.2 Description of Continia Software

Continia was established in 2009, and the group has 128 employees with many subsidiaries worldwide.


The foundations of Continia were laid by the company Hotcom A/S in 1993 when that company developed a software product, NaviBanking, to make day-to-day bank-related tasks easier for employees of finance departments. In 1999, Hotcom changed its name to Celenia Software, and the company also provided time-based service to its customers.

In 2009, a few Celenia Software employees and some external investors formed the company Continia Software A/S. At the same time, Continia acquired the product-related business of Celenia, including customers. One of these former Celenia employees was Henrik Lærke, the Head of Department at Celenia, who became the CEO of Continia. Henrik Lærke is still the present CEO of Continia.

During the last 5 years, Continia has established fully owned subsidiaries and offices in The Netherlands, Belgium, Germany, the USSpain, and Lithuania. Continia strives to be a global leader in its market with a local presence. The success of Continia is highly attributed to a strong Microsoft partner channel worldwide that also sells and implements Continia products to its customers.

Since the beginning, Continia has developed and acquired more software products focusing on streamlining the processes in finance departments. Most of Continia's products are installed as add-ons to its customers' own Microsoft Dynamics 365 Business Central ERP system. These customers are typically within the SME segment (5-200 employees) but also include some larger organizations with, e.g., decentralized implementations in subsidiaries.

As technology evolves, Continia's products increasingly use online services for OCR processing, communication with banks, integration to electronic invoicing networks, mobile devices, etc. Continia also uses online services to monitor the use of the products with a strong focus on implementing improvements. Collectively, these services are called Continia Online Services.



Continia's focus is to provide secure, reliable products that support customers' demands, laws, and regulations. To support this, Continia established an IT Security Project in 2016, which is the basis of the company's security strategy and security activities.

### 2.3 Business strategy / IT security strategy

Continia's strategy is to incorporate sufficient internal security measures and standards to avoid the company being exposed to unacceptable risks. As a software provider to companies worldwide, we work with IT security at a business-strategic level. We want to be a professional software provider with a sharp attitude toward protecting the data the customers have entrusted to us.

In Continia, we want to ensure compliance with current legislation and do what is technically and financially possible to secure a high level of confidentiality, integrity, and accessibility of data processing.

IT security is paramount at all levels of the organization. All employees within Continia must understand the importance of this focus, and they themselves must adapt and contribute to improving IT security.

Our aim regarding IT security is that Continia undertakes all necessary activities to ensure:

- **Accessibility** to Continia Online Services: to achieve a high degree of accessibility with a high up-time rate and minimized risk of breakdown.
- **Integrity**: to achieve a reliable and correct function of Continia Online Services and a minimized risk of using incorrect data e.g., because of human or system-related errors or external incidents.
- **Confidentiality**: to ensure confidential data processing, transmission, and storage of data, only accessible by authorized users.

It is Continia's intent to maintain a level of information security which as a minimum:

- Complies with current laws and regulations.
- Implement generally accepted practices of the industry.
- Meets the customers' requirements and expectations of a professional software provider.

To ensure a uniform delivery, we have decided that the operations of Continia Online Services are subject to an audit procedure aiming to meet the demands of an ISAE3402 report. The audit procedure is repeated annually, and results are included in an Auditor's Report made public on our website [www.continia.com](http://www.continia.com).

The Auditor's Report will contribute to the customer's (*the Data Controller's*) control, whether Continia lives up to the directions laid down in the Data Processor Agreement with the customer.

Continia has decided to base its IT security strategy on ISO27001 + 2 and is thus applying the ISO methodology to implement relevant security measures within the following areas:

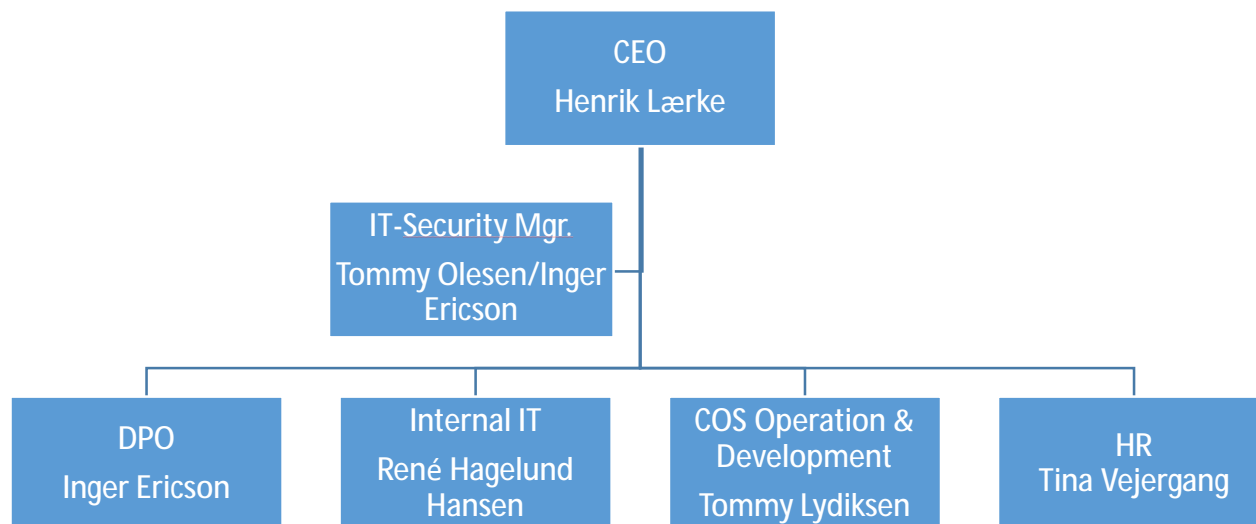
- Information security policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Physical and environmental security
- Operations security

- Communication security
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance with legal and contractual requirements

The security measures implemented by Continia are listed in Appendix 1 to this description.

## 2.4 Continia organizorganization and organizorganizing of IT security

Continia's IT Security Team is organized according to the following structure:



CEO – develops Strategies and Goals and has the overall responsibilities regarding IT Security.

IT Security Team is responsible for the IT Security Project, the procedures, follow-up, and documentation regarding IT security, as well as for ensuring a continuous development of IT security at Continia.

HR handles employment, development, and dismissal of staff, as well as accompanying documents and communication.

COS Operation & Development takes care of the operations of Continia Online Services i.e. deployment, monitoring, backup, updates as well as develops new functionalities to Continia Online Services


DPO is responsible for compliance and act as a contact point for internal and external stakeholders regarding privacy and general governance.

At Continia, we have appointed an IT Security Team, and its aim is to ensure that our security is sufficient within the following areas:

- ✓ Operation of IT services
- ✓ Access
- ✓ Contingency measures
- ✓ Staff behaviour
- ✓ Backup
- ✓ Network
- ✓ Monitoring
- ✓ Encryption
- ✓ Security measures against malicious programs (Spam filtering, Antivirus etc.)
- ✓ Compliance
- ✓ Control procedures

The IT Security Team is directly responsible to the CEO. The organizational deployment of the IT security (incl. Information security) is in this way a natural part of the Management's responsibility.

Continia applies a structured method to ensure that all relevant procedures and policies are described in our IT Security Manual. This is to ensure that we do not depend on a specific individual and can replace employees without any loss of critical know-how to the production environments. Incidents and



deviations relating to our IT security are registered in an internal task system to ensure documentation and follow-up on deviations.

Deployment of the IT security is ensured by the establishment of IT Security Team working with awareness, rules, and procedures.

## 2.5 Risk management at Continia

Continia's policy for the risks related to the company's security activities is to be covered or limited to such an extent that the company will always have the capacity to maintain normal operations.

As part of the IT Security Strategy mentioned above, Continia works with the IT security standard ISO27001 + 2, constituting our IT security's primary framework. Work relating to IT security is a continuous and dynamic process designed to ensure that we adapt to changing requirements, new risks arising, and general expectations from our customers.

In Continia, we perform an ongoing risk assessment of our business, especially Continia Online Services. This enables us to minimize risks associated with our services to an acceptable level. Risk assessment is performed periodically, and as a minimum when we make changes or implement new systems and services. Risk assessment is part of the IT Security Team's responsibility and must subsequently be deployed to and approved by the company's Management.

## 2.6 Managing IT security

The management of Continia has the day-to-day responsibility for IT security, and thus, it is ensured that the overall requirements and framework for IT security are complied with. Management has described Continia's structure for IT security of Continia Online Services through the IT Security Manual. The IT security policies and the manual must as a minimum be revised once a year.

Continia's IT Security Manual considers the items mentioned above and applies to all employees and deliveries relating to Continia Online Services. Any security breach or incident in our operating environment will be considered with the highest priority and invoke our emergency response and plan immediately. We follow standard procedures to ensure traceability, preventive, and corrective actions.

The IT Security Manual provides Continia with a standard set of rules, that allows us to obtain stable operating environments and a high security level. We make regular improvements to policies, procedures, and operations.


In the area of overall IT security Continia has implemented the necessary procedures and control measures relating to each of the areas within ISO27001 + 2 as defined in Appendix 1, showing the security structure and the control objectives implemented at Continia.

## 2.7 HR, employees, and training

Our employees are one of our most important assets, and we implement structured ways to ensure employees' qualifications, relevant training, and certifications. We use annual talks about continuous training/further studies, where we decide the objectives for the employees' professional development based on their wishes.

In our HR Department we work according to standard procedures for recruitment, employment, and termination of employment. New employees are subjected to a thorough company introduction procedure. The procedure includes information about information security, dealing with IT security rules, introduction to our information security organization, appropriate IT behavior, classification of data, and focus on Continia's role as data processor.





Continia's employees have the possibility to work from other premises than their local office. The company has devised a procedure describing rules and advice regarding remote working. We have established technical measures ensuring encrypted online access to office facilities. Access to back-end systems and operating environments is limited.

All employment contracts include a confidentiality clause. As part of our end-of-employment procedure, an exit conversation with the employee's immediate manager is included. During this conversation, we emphasize that the confidentiality clause is still in effect after the end of employment.

To ensure our information security culture, we provide ongoing information and execute periodic tests to assess the IT security knowledge of our employees. The information and results are re-assessed annually by the IT Security Team.

## 2.8 Physical and environmental security

Continia uses one main external supplier in connection with COS: Microsoft Azure for COS operation hosting. It means we have entrusted the basic COS data center assignments to the supplier.

The supplier is responsible for physical security, fire and water detection and fighting, as well as power and cooling. The supplier's data centers provide several layers of security and meet the requirements of generally accepted international standards for information security regarding management systems and business continuity management.

### *Controlling suppliers*

For suppliers to critical parts of our operations environment, Continia controls every year (as a minimum), whether the suppliers meet the requirements and SLA in relation to the services they provide. Continia evaluates each supplier's certifications, audit reports etc. and compares them with our own observations. From that we assess, whether the supplier lives up to the agreed services, and whether there is reason to bring up certain aspects with them.

## 2.9 Operating Continia Online Services

Standard operational tasks are carried out according to standard intervals. Such tasks are managed by Continia's COS Operations Department conducting controlled maintenance and operation of all servers.

### *IT production equipment*


Continia documents its IT equipment in the Microsoft System Management. The purpose is always to maintain a database updated with relevant data about IT equipment and an updated antivirus /operating system.

IT equipment with an IP-address that is directly, or indirectly, part of production environments and/or office environments must be documented and kept updated in the Microsoft security systems when possible. This includes network equipment, servers (physical/virtual), printers, PCs, mobile devices, applications, operation systems, services, and databases.

### *Monitoring of operations – Continia Online Services*

Our operations environments are constantly monitored by using automated monitoring services. Resources for servers are monitored (CPU, ram, disc, network) as well as accessibility. Monitoring also includes relevant IT services like backups, accessibility for customer facing systems and systems for internal use.

Monitoring is primarily targeted at our own environments, but also includes some external environments and services that are part of selected COS services.



In case of an incident, it is reported to COS Operations, who investigate and plans accordingly. In the event of a critical incident, the operator on duty is alerted directly.

When relevant, we provide updates to our status and operation on our public status page (<http://statuspage.continia.com>). Customers, who experience issues related to our operations, can also get support and updates by the agreed channels in their contracts or according to Service License Terms (EULA).

#### *Logging*

We use logging for monitorization and troubleshooting. As log data contain various information, we incorporate access management to ensure employees can only access what they need. We implement logging on several levels, such as application logging to log relevant events in our applications, and access logging to document when users or systems access our applications.

#### *Backup*

The purpose of backup is to ensure that we can restore systems and customer data in an accurate and timely manner, when necessary. We perform backup on multiple levels, such as virtual servers, configurations, and data, which provide us with a variety of options if we need to reestablish a service or data.

We perform backup of relevant databases and configurations, which allows us to restore data and services in case of an emergency. There are different demands to the frequency of backups, which depends on the criticality of the service or application.

Our backup policy for customer data requires us to perform daily backup of customer data. All backups are stored at location that is physically separated from the operational location.

#### *Patch management*

The purpose of patch management is to ensure that all relevant updates such as patches, fixes and service packs from suppliers are implemented to protect systems against known threats, downtime, and unauthorized access. This also ensures that the implementation is done in a controlled manner.

Maintenance of Windows operating systems and accompanying back-end systems from Microsoft, is managed by Microsoft's integrated WSUS (Windows Server Update Services), where security and critical patches are installed automatically at standard intervals.

## **2.10 Managing information security incidents**


Security incidents and identified weaknesses in Continia Online Services must be reported in a way that makes it possible to perform remedial action in a timely manner. Procedures for incident management and deviation reporting, including security breaches, are established to ensure that work is performed systematically and relevant data and documentation is collected to allow subsequent evaluation.

## **2.11 User management / access security**

The purpose of user management is ensuring that only authorized users have access to the systems.

When we grant access or permissions to operational environments and data, we always consider business related objectives and the classification of information. Physical, as well as logical access, is based on the principles "need-to-know" and "least privilege", meaning that access is only granted when needed to perform one's tasks, job or role.

Granting of access or permissions to internal IT systems and production environments follows standard procedure to ensure segregation of request, approval, verification, and implementation. Access management is documented in a central system.



We have implemented a hardened password policy dictating long complex passwords and multi-factor authentication.

## 2.12 Emergency response management

At Continia, our main business is to provide products, and often related online services in COS to customers. Therefore, our IT emergency response is also regarded as an overall business continuity plan.

In case of major incident, the IT Security Team and Management are informed. As soon as possible, we appoint a person in charge of the situation, who is also responsible for coordinating our response to the incident, communication plan, and remediation.

We perform a yearly review and quality assurance of all re-establishment plans. In addition, we perform a yearly desk test of one or more selected systems.

## 2.13 Development environment

When we develop and test new software (new functionality for Continia Online Services), we use dedicated test environments that are separated from our production environments used by customers. Both development and test environments are isolated by its own IP segment.

Any potential errors in data or system integrations is limited to impact other test data and not production data. During development and testing we work with fictional data and therefore not real customer data. Although, during the final stages testing, there might be a need for test data resembling data from production environments.

We implement a set of standard procedures for development, test and approval in our development teams. Before any code is deployed to our operation environments it has always been through a code review by another developer.

Access to databases in COS is limited and can only be accessed from the outgoing IP-addresses of our Aalborg and Copenhagen office.

## 3. Compliance with the role as Data Processor

Continia's Management is responsible for identifying and ensuring compliance with all relevant legal and contractual requirements, e.g.:


- The EU General Data Protection Regulation
- The Danish Data Protection Act
- Continia – License and Term of Service Agreement (EULA)
- Continia – Data Processor Agreement

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.

Furthermore, Continia's IT Security Team reviews all our security policies on a regular basis, involving any relevant stakeholders. Continia's ISMS is regularly audited by an independent, external party, and on request the audit report is shared with all Continia's customers.

### 3.1 The EU General Data Protection Regulation (GDPR)

According to the EU General Data Protection Regulation, Continia is the Data Processor, and the customer is the Data Controller.



Continia ensures that all legal requirements are identified and accommodated. Continia 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, Continia 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 ISO27001 + 2 standard ensures an appropriate security level. Besides compliance with the relevant ISO requirements, Continia ensures data privacy and data security on a contractual level.

### 3.2 Privacy and protection of personal data

As mentioned above, Continia is the customers' Data Processor, given that the customers are using Continia Online Services. Continia is not responsible for any data uploaded by the customers to their Continia Online Service. Continia ensures that data uploaded by the customers are sufficiently protected. Below is a description of Continia's procedures for operating as a Data Processor, following directions from the customers i.e., the Data Controllers.

#### *Data Protection Agreements*

Continia provides standard Data Processor Agreements to all our customers. These contracts outline Continia's role and responsibilities as Data Processor. According to standard Data Processor Agreement, Continia keeps data records aimed to our customers' activities divided according to software products:

- The name and contact information of suppliers, sub-processors, and customers.
- The categories of processing carried out by the suppliers or any sub-processors on behalf of the customer.
- No transfer of any personal data outside of EEA.
- Where possible, a general description of the technical and organizational security measures undertaken by the supplier to safeguard personal data.

### 3.3 Access to data in customer instances

In general, Continia can access any customer instances specifically instructed by the customer. Continia does not collect data about the customer's customers (recipients).

On request from a customer, Continia can use recipients' personal data to:


- help and train the customer to use Continia Online Services solutions (customer support).
- investigate issues related to the customer's recipients (e.g. in case of reported errors).
- set up a user to Continia Online Services according to the customer's instructions.
- other relevant actions, on request from the customer.

In short, Continia can access data collected by the customer, but only accesses it, upon instructions by the customer. Only selected employees at Continia have access to the customer's data and can access it upon the customer's request. Continia is required to disconnect the access to the customer's data immediately after this access is no longer necessary.

Continia logs and monitors the access to the customers' data in Continia Online Services to ensure that no unauthorized persons get access.

### Customers' responsibilities (complementary controls at the customer)

This Chapter describes the general control environment for Continia Online Services, which means that no account has been made for the agreements of individual customers.



Continia is not responsible for access rights, including granting, changing and removal, in relation to the individual customer's users and their access to Continia Online Services. The customer is responsible for ensuring any controls necessary in connection with this control objective.

Customers are responsible for data transmission to Continia Online Services, and it is the customers' responsibility to create the necessary data transmission.

## APPENDIX 1:

# Continia applies the following control objectives and security measures from ISO27001 and 2

### 0. Risk Assessment and management

- 0.1. Assessment of security risks
- 0.2. Risk management

### 5. Information security policies

- 5.1. Management directions for information security

### 6. Organizing of information security

- 6.1. Internal organization
- 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. Handling of media

### 9. Access control

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

### 11. Physical and environmental security

- \*\* Limited responsibility\*\*
- 11.1. Secure areas
- 11.2. Equipment

### 12. Operations security

- \*\* Limited responsibility\*\*
- 12.1. Operational procedures and responsibilities
- 12.2. Protection from malware
- 12.3. Backup
- 12.4. Logging and monitoring
- 12.5. Operational software management

### 13. Communications security

- \*\* Limited responsibility\*\*
- 13.1. Network security management

### 14. (Acquisition), development and maintenance of systems

- 14.1. Security requirements to the IT system

### 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

#### \*\* Limited responsibility \*\*

Responsibility for compliance with the control objective is divided between Continia and the subcontractors.

See description of controls in relation to covering the control risk, including how Continia continually supervises operations security and data security at subcontractors.

## CHAPTER 3:

# Independent auditor's assurance report on the description of controls, their design and operating effectiveness

For the customers / users of Continia Online Services and their auditors

### Scope

We have been engaged to report on Continia's description in Chapter 2 (incl. Appendix 1), which is a description of the control environment in connection with the operations of Continia Online Services, see Data Processor Agreements with customers, throughout the period 1 May 2022 – 30 April 2023, as well as on the design and function of controls regarding the control objectives stated in the description.

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. The report does not include control or supervision of subcontractors in relation to operation activities. Continia's subcontractors are listed in the Data Processing Agreements with the customers.

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: Customers' responsibilities.

### Continia's responsibility

Continia is responsible for the preparation of the description and accompanying assertion in Chapter 2 (including Appendix 1), including the completeness, accuracy, and method of presentation of the description and assertion; for providing the services 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 ISQM 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, based on our procedures, on Continia's description and on the design and operation of controls related to the control objectives stated in the said description. We have conducted our engagement in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organization, 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 in all material aspects are appropriately designed and operate effectively.



An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and about the design and operating effectiveness of controls. The procedures selected depend on the judgement of the service organization's auditor, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or not operating effectively.

Our procedures included testing the operating effectiveness of such controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. 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 by Continia in Chapter 2 (including Appendix 1).

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

### Limitations of controls at Continia

Continia'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 their own environment. Moreover, because of their nature, controls at Continia may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at the service organization may become inadequate or fail.

### 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 Continia's control environment for the operation of Continia Online Services, such as it was designed and implemented throughout the period 1 May 2022 – 30 April 2023 in all material respects; and
- b) The controls related to the control objectives stated in the description were in all material respects suitably designed throughout the period 1 May 2022 – 30 April 2023; and
- c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved in all material respects, had operated effectively throughout the period 1 May 2022 – 30 April 2023.


### Description of tests of controls

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

### Intended users and purpose

This report and the description of the test of controls in Chapter 4 are solely intended for Continia's customers and their auditors, who have sufficient understanding to consider them along with other information, including information about the customers' own control measures, which the customers as Data Controllers have performed themselves, when assessing compliance with the demands to the control environment as well as with the requirements of the General Data Protection Regulation.






Søborg, 10 July 2023

**Beierholm**  
Statsautoriseret Revisionspartnerselskab  
CVR 32 89 54 68



Kim Larsen  
State-authorized Public Accountant



Jesper Aaskov Pedersen  
IT-auditor, Director

# Auditor's description of control objectives, security measures, tests, and findings

We have structured our engagement in accordance with ISAE 3402 – Assurance Reports on Controls at a Service Organization. For each control objective, we start with a brief summary of the control objective as described in the frame of reference ISO27001 and 27002: 2017.

With respect to the period, we have tested whether Continia has complied with the control objectives throughout the period 1 May 2022 – 30 April 2023.

Below the grey field are three columns:

- The first column tells the activities Continia, according to their documentation, has put into practice in order to comply with the requirements.
- The second column tells how we have decided to test, whether facts tally with descriptions.
- The third column tells the findings of our test.

## The Tests Performed

The tests performed in connection with establishing the control measures' design, implementation, and operational efficiency are conducted using the methods described below:

Inspection	Reading of documents and reports containing information about execution of the control. This includes, inter alia, reading and deciding about reports and other documentation in order to assess, whether it can be expected that the design of specific control measures will be efficient, if implemented. Furthermore, it is assessed whether control measures are monitored and controlled sufficiently and with appropriate intervals.
Enquiries	Enquiries to/interview with relevant staff at Continia. Enquiries have included how control measures are performed.
Observation	We have observed the performance of the control.
Repeating the control	Repeated the relevant control measure. We have repeated the performance of the control in order to verify that the control measure works as assumed.

## Risk Assessment and Management

The risk assessment must identify and prioritise the risks based on the operation of Continia Online Services. The findings are to contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Through a risk assessment, risks have been identified and prioritised. The Continia Online Services defined in the description are used as basis for the assessment.</p> <p>The findings contribute to the identification and prioritisation of management interventions and security measures necessary to address relevant risks.</p>	<p>We have requested and obtained the relevant material in connection with the audit of risk management.</p> <p>We have checked that regular risk assessments are carried out for Continia Online Services in relation to business conditions and their development. We have checked that the risk assessment is deployed down through the company's organization.</p> <p>We have checked that the company's exposure is managed on a current basis and that relevant adaptations of consequences and probabilities are made regularly.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 5:

## Information Security Policies

Management must prepare an information security policy that covers, among other things, management's security objectives, policies, and overall action plan. The information security policy is maintained, taking the current risk assessment into consideration.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>There is a written strategy covering, among other things, Management's security objectives, policies, and overall action plan.</p> <p>The IT security policy and accompanying supporting policies are approved by the company's Management, and then deployed down through the company's organization.</p> <p>The policy is available for all relevant employees.</p> <p>The policy is re-evaluated according to planned intervals.</p>	<p>We have obtained and audited Continia ' latest IT security policy.</p> <p>During our audit, we checked that maintenance of the IT security policy is conducted on a regular basis. At the same time, we checked during our audit that the underlying supporting policies have been implemented.</p> <p>We have checked that the policy is approved and signed by the company's Supervisory and Executive Boards and made available for the employees on Continia ' intranet.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 6:

## Organization of Information Security

Management of the IT security must be established in the company. Organizational responsibility for the IT security must be placed with appropriate business procedures and instructions. The person responsible for IT security must, among other things, ensure compliance with security measures, including continuous updating of the overall risk assessment.

In relation to the use of mobile devices and/or teleworking, Management must ensure a suitable level of protection for teleworking and the use of mobile devices.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Organizational responsibility for IT security has been placed, documented, and implemented.</p> <p>The IT security has been coordinated across the company's organization.</p>	<p>Through inspection and tests, we have ensured that the organizational responsibility for IT security is documented and implemented.</p> <p>We have checked that the IT security is deployed across the organization in relation to Continia Online Services.</p> <p>By making interviews, we have checked that the person responsible for IT security knows his/her role and responsibilities.</p>	<p>No comments.</p>
<p>Risks in relation to use of mobile devices and teleworking have been identified.</p>	<p>We checked that formal policies exist in connection with the use of mobile devices and teleworking.</p> <p>On a test basis, we have inspected that the policy is implemented regarding employees using mobile devices.</p> <p>Regarding the use of teleworking at Continia, we have checked whether appropriate security measures have been implemented thus this area is covered in relation to the risk assessment of the area.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 7:

## Human Resource Security

It must be ensured that all new employees are aware of their specific responsibilities and roles in connection with the company's information security in order to minimise the risk of human errors, theft, fraud and abuse of the company's information assets.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Based on the specified work processes and procedures, it is ensured that all new employees are informed of their specific responsibilities and roles in connection with their employment at Continia. This includes the framework laid down for the work and the IT security involved.</p> <p>Security responsibilities, if any, are determined and described in job descriptions and in the form of terms and conditions in the employment contract.</p> <p>The employees are familiar with their professional secrecy based on a signed employment contract and through Continia ' HR policy.</p>	<p>We have verified that routines and procedures developed by Management in connection with start of employment and termination of employment have been adhered to.</p> <p>Based on random samples, we have tested whether the above routines and procedures have been complied with in connection with start of employment and termination of employment.</p> <p>Through interviews, we have checked that employees of significance to Continia Online Services are familiar with their professional secrecy.</p> <p>We have examined the job descriptions and employment contracts of key employees and subsequently tested the awareness of the individual employee of their roles and related security responsibility.</p> <p>We have ensured that Continia ' HR policy is easily accessible and has a section on terms for professional secrecy with respect to information obtained in connection with work conducted at Continia.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 8:

## Asset Management

Necessary protection of the company's information assets must be ensured and maintained, all the company's physical and functional assets related to information must be identified, and a responsible owner appointed. The company must ensure that information assets related to Continia Online Services have an appropriate level of protection.

There must be reassuring controls to ensure that data media are properly disposed of when no longer needed, in accordance with formal procedures.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>All information assets have been identified and an updated list of all significant assets has been established.</p> <p>An "owner" of all significant assets is appointed in connection with the operation of Continia Online Services.</p>	<p>We have examined and checked the company's central IT register for significant IT entities in connection with the operation of Continia Online Services. Through observations and control, we checked relations to central knowhow systems for the operation of Continia Online Services.</p> <p>By observations and enquiries, we have checked that Continia complies with all material security measures for the area in accordance with the security standard.</p>	<p>No comments.</p>
<p>Information and data in relation to Continia Online Services and the subsequent operation of the solution are classified based on business value, sensitivity and need for confidentiality.</p>	<p>We have controlled that there is an appropriate division of assets and accompanying procedures for Continia Online Services. In this connection, we have controlled, whether internal procedures/routines regarding ownership to applications and data are complied with.</p> <p>We have checked that contracts and SLA are used as central tools to ensure the definition, segregation, and delimitation of Continia ' responsibilities and the customer's responsibilities with respect to access to information and data.</p> <p>Accordingly, the customer is typically responsible for ensuring that a suitable protection level exists for own information and data.</p>	<p>No comments.</p>
<p>Procedures for dealing with destruction of data media are established.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>• Asked Management which procedures/ control activities are performed regarding destruction of data media.</li> <li>• On a sample basis gone through the procedures for destruction of data media.</li> </ul>	<p>No comments.</p>

CONTROL OBJECTIVE 9:

## Access Control

Access to the company's systems, information and network must be controlled based on business and statutory requirements. Authorised users' access must be ensured, and unauthorised access must be prevented.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Documentation and updated directions exist for Continia ' access control.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management, whether access control procedures have been established at Continia.</li> <li>verified on a test basis that access control procedures exist and have been implemented; see Continia ' directions.</li> <li>by interviewing key staff and by inspection on a test basis, we have verified that access control for the operations environment comply with Continia ' directions, and authorisations are granted according to agreement.</li> </ul>	<p>No comments.</p>
<p>A formal business procedure exists for granting and discontinuing user access.</p> <p>Granting and application of extended access rights are limited and monitored.</p>	<p>We have by inspection on a test basis verified:</p> <ul style="list-style-type: none"> <li>that adequate authorisation systems are used in relation to access control at Continia.</li> <li>that the formalised business procedures for granting and discontinuing user access have been implemented in Continia ' systems, and registered users are subject to regular follow-up.</li> </ul>	<p>No comments.</p>
<p>Internal users' access rights are reviewed regularly according to a formalised business procedure.</p>	<p>By inspection on test basis, we have verified that a formalised business procedure exists for follow-up on authorisation control according to the directions, including:</p> <ul style="list-style-type: none"> <li>that formal management follow-up is performed on registered users with extended rights every 6 months.</li> <li>that formal management follow-up is performed on registered users with ordinary rights every 12 months.</li> </ul>	<p>No comments.</p>



<p>The granting of access codes is controlled through a formalised and controlled process, which ensures, among other things, that standard passwords are changed.</p>	<p>We have asked Management whether procedures granting access code have been established at Continia.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>• that an automatic systems control takes place, when access codes are granted to check that passwords are changed after first login.</li> <li>• that standard passwords are changed in connection with implementation of systems software, etc.</li> <li>• if this is not possible, that procedures ensure that standard passwords are changed manually.</li> </ul>	<p>No comments.</p>
<p>Access to operating systems and networks are protected by passwords.</p> <p>Quality requirements have been specified for passwords, which must have a minimum length (6 characters), requirements as to complexity, maximum duration (max 365 days), and likewise password setup means that passwords cannot be reused (remembers the latest 24 versions).</p> <p>All employees are forced to use multi-factor authentication.</p> <p>Furthermore, the user will be barred, in the event of repeated unsuccessful attempts to login.</p>	<p>We have asked Management whether procedures ensuring quality passwords in Continia are established.</p> <p>By inspection on a test basis, we have verified that appropriately programmed controls have been established to ensure quality passwords complying with the policies for:</p> <ul style="list-style-type: none"> <li>• minimum length of password</li> <li>• complexity of password</li> <li>• maximum life of password</li> <li>• minimum history of password</li> <li>• multi-factor authentication</li> <li>• lockout after unsuccessful login attempts</li> </ul>	<p>No comments</p>

CONTROL OBJECTIVE 12:

## Operations Security

Control objective: Operations procedures and areas of responsibility.

A correct and adequate running of the company's operating systems must be ensured. The risk of technology related crashes must be minimised. A certain degree of long-term planning is imperative in order to ensure sufficient capacity. A continuous capacity projection must be performed based on business expectations for growth and new activities and the capacity demands derived hereof.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>The operations procedures for business-critical systems are documented, and they are available to staff with work-related needs.</p> <p>Management has implemented policies and procedures to ensure satisfactory segregation of duties.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>• Asked Management whether all relevant operation procedures are documented.</li> <li>• In connection with our audit of the individual areas of operation verified on a test basis that documented procedures exist and that there is concordance between the documentation and the procedures actually performed.</li> <li>• Inspected users with administrative rights in order to verify that access is justified by work-related needs and does not compromise the segregation of duties.</li> </ul>	<p>No comments.</p>
<p>Management of operational environment is established in order to minimise the risk of technology related crashes.</p> <p>Continuous capacity projection is performed based on business expectations for growth and new activities and the capacity demands derived hereof.</p>	<p>We have:</p> <p>Asked Management about the procedures and control activities performed.</p> <p>On a test basis examined that the operation environment's consumption of resources is monitored and adapted to the expected and necessary capacity requirements.</p>	<p>No comments.</p>

Control objective: Protection from malware

To protect from malicious software, such as virus, worms, Trojan horses, and logic bombs. Precautions must be taken to prevent and detect attacks from malicious software.

Continia ' control procedures	Auditor's test of control procedures	Test findings
Preventive, detecting and remedial security and control measures have been established, including the required training and provision of information for the company's users of information systems against malicious software.	<p>We have:</p> <ul style="list-style-type: none"> <li>enquired about and inspected the procedures/ control activities performed in the event of virus attacks or outbreaks.</li> <li>enquired about and inspected the activities meant to increase the employees' awareness of precautions against virus attacks or outbreaks.</li> <li>verified that anti-virus software has been installed on servers and inspected signature files documenting that they have been updated.</li> </ul>	No comments.

Control objective: Backup

To ensure the required accessibility to the company's information assets. Set procedures must be established for backup and for regular testing of the applicability of the copies.

Continia ' control procedures	Auditor's test of controls	Test findings
Backup is made of all of the company's significant information assets, including e.g., parameter setup and other operations-critical documentation, according to the specified directions.	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management about the procedures/ control activities performed.</li> <li>examined backup procedures on a test basis to confirm that these are formally documented.</li> <li>examined backup log on a test basis to confirm that backup has been completed successfully and that failed backup attempts are handled on a timely basis.</li> <li>examined physical security (e.g., access limitations) for internal storage locations to confirm that backup is safely stored.</li> </ul>	No comments.

Control objective: Logging and monitoring

To reveal unauthorised actions. Business-critical IT systems must be monitored, and security events must be registered. Logging must ensure that unwanted incidences are detected.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Operating systems and network transactions or activities involving special risks are monitored. Abnormal conditions are examined and resolved on a timely basis.</p> <p>Continia logs when internal users log off and on the systems.</p> <p>Only in the event of suspected or identified abuse of the systems, users are actively monitored.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management about the procedures/ control activities performed and have examined the system setup on servers and important network units as well as verified that parameters for logging have been set up, thus transactions made by users with extended rights are being logged.</li> <li>checked on a test basis that logs from critical systems are subject to sufficient follow-up.</li> </ul>	<p>No comments.</p>
<p>A central monitoring tool is used which sends alerts, if known errors occur. If possible, it is monitored whether an error is about to occur in order to react proactively.</p> <p>Alerts are shown on the monitoring screen mounted in the project and operations department. Critical alerts are also sent by email and SMS.</p> <p>Status reports are sent by email from different systems. Some daily – others when incidents occur in the system. The operator on duty is responsible for checking these emails daily.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management about the procedures/ control activities performed.</li> <li>ensured that a monitoring tool is used and that this is available to all employees.</li> <li>ensured that alerts are sent by email and SMS, if errors occur.</li> <li>examined status reports.</li> <li>ensured that an operator on duty is established and that this operator on duty checks reports on a daily basis.</li> </ul>	<p>No comments.</p>

Control objective: Managing operations software

Ensuring establishment of appropriate procedures and controls for implementation and maintenance of operating systems.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Changes in the operation environment comply with established procedures.</p>	<p>We have asked Management, whether procedures for patch management are established in Continia.</p> <p>By inspection on test basis, we have verified that</p> <ul style="list-style-type: none"> <li>• adequate procedures are applied, when controlled implementation of changes to the production environment of Continia is performed.</li> <li>• changes to Continia ' operation environment comply with directions in force, including correct registration and documentation of applications about changes.</li> </ul> <p>On a test basis, we have inspected that the operating systems are updated in compliance with procedures in force and that current status is registered.</p>	<p>No comments.</p>
<p>Changes in existing user systems and operation environments comply with formalised procedures and processes.</p>	<p>We have asked Management, whether procedures for patch management are established in Continia.</p> <p>By inspection on test basis, we have verified that adequate procedures are applied for controlled implementation of changes in the production environments, including that demands to the patch management controls ensure that</p> <ul style="list-style-type: none"> <li>• applications for change are registered and described.</li> <li>• all changes are subject to formal impact assessments before implementation.</li> <li>• All changes are subject to formal impact assessments.</li> <li>• fall-back plans are described.</li> <li>• systems affected by changes are identified.</li> <li>• Documented test of changes is performed before putting into operation</li> <li>• documentation is updated reflecting the implemented changes in all material respects.</li> <li>• procedures are subject to managing &amp; coordination by a "Change Board"</li> </ul>	<p>No comments.</p>

CONTROL OBJECTIVE 13:

# Communications Security

To ensure protection of information in networks and support of information processing facilities.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Networks must be protected against threats in order to secure network-based systems and the transmitted data.</p> <p>Production environment must be secured against failing supply in relation to redundancy to network connection to the internet.</p> <p>Network traffic/access from production environment to the outside world is available by means of multiple supply entries or access from more than one supplier.</p>	<p>It has been checked that necessary protection against unauthorised access is implemented, including:</p> <ul style="list-style-type: none"> <li>• Appropriate procedures for managing network equipment are established.</li> <li>• Segregation of user functions is established.</li> <li>• Appropriate logging and monitoring procedures are established.</li> <li>• Managing the company's network is coordinated in order to ensure optimal utilisation and a coherent security level.</li> <li>• Ensured that connections for data communication with the internet are established via more than one ISP supplier.</li> <li>• On a sample basis gone through documentation from the suppliers about written basis for contract, as well as regular settlement of accounts for services rendered by the ISP suppliers.</li> </ul>	<p>No comments.</p>
<p>Adequate procedures for managing threats in the form of attacks from the internet (cyber-attacks) must be implemented.</p> <p>In this connection, tools for managing the contingency approach in the event of a cyber-attack must be devised.</p>	<ul style="list-style-type: none"> <li>• We have controlled that an adequate number of procedures with accompanying contingency plans regarding managing threats in relation to cyber-attacks are implemented.</li> </ul> <p>By inspection on a test basis, we have ensured:</p> <ul style="list-style-type: none"> <li>• that appropriate framework for managing cyber-attacks is devised.</li> <li>• that plans for managing the threat are devised and implemented.</li> <li>• that the plans include cross-organizational collaboration between internal groups.</li> </ul>	<p>No comments.</p>

## (System acquisition), development and maintenance

Ensure that Continia Online Services are managed using suitable IT security measures, including appropriate segregation of production and development environment.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Continia has planned system development and maintenance activities based on the proprietary model for project management.</p> <p>The structure of the development organization includes a central steering committee responsible for providing suitable work routines and accompanying control measures for the management.</p> <p>All changes meant to be put into operation in the production environment, must be approved by the development group for each of the Continia Online Services.</p> <p>Software development must be placed in independent test environments.</p>	<p>We have:</p> <ul style="list-style-type: none"> <li>asked Management, whether a general quality management model for managing software development is devised or does exist.</li> <li>in connection with the audit checked the existence of procedures and routines for rolling out software changes.</li> </ul> <p>In connection with our audit, we have checked that internal education is conducted for staff working with development of Continia Online Services and the accompanying development environment. During the process we tested whether staff was trained in using quality model for development</p> <p>The control environment for the development platform is based on the same IT security structure as stated for the production environment.</p> <p>User management ensures suitable control measures in connection with managing the logical access control. We have checked that the different user groups are controlled at set intervals.</p> <p>The structure of the development organization includes a central steering committee responsible for providing suitable work routines and accompanying control measures for the management.</p> <p>We have on a sample basis checked that all user activities are recorded and logged in the central database. The person responsible for IT security reviews the log database on a regular basis.</p> <p>We have checked the existence of procedures for segregation of the production environment and the environment for development and maintenance.</p> <p>We have on a sample basis tested that the production environment for software development is conducted from an independent IP segment.</p>	<p>No comments.</p>

CONTROL OBJECTIVE 15:

## Supplier Relationships

External business partners are obliged to comply with the company's established framework for IT security level.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Risks related to external business partners are identified, and security in relation to agreements with third parties are managed.</p>	<p>We have verified that in connection with the use of external business partners there are formal cooperation agreements.</p> <p>On a test basis, we have inspected that the cooperation agreements with external suppliers comply with the requirements about covering relevant security conditions in relation to the individual agreement.</p>	<p>No comments.</p>
<p>In case of changes with impact on the production environment, and where services from external suppliers are used, suppliers are selected through collaboration between the Operations Manager and the IT Security Manager. Solely approved suppliers are used.</p>	<p>We have asked Management about relevant procedures applied in connection with selecting external partners.</p> <p>We have ensured that appropriate procedures for managing cooperation with external partners are established.</p> <p>We have tested that key suppliers have updated and approved contracts.</p>	<p>No comments.</p>
<p>Monitoring must be conducted on a regular basis, including supervision of external business partners.</p>	<p>We have ensured that there are appropriate processes and procedures for ongoing monitoring of external suppliers.</p> <p>We have checked that ongoing supervision is conducted by means of independent auditor's reports.</p>	<p>No comments.</p>



CONTROL OBJECTIVE 16:

## Information Security Incident Management

To achieve reporting of security incidents and weaknesses in the company's information processing systems in a way that allows for timely corrections.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>Security incidents are reported to Management as soon as possible, and the handling is performed in a consistent and efficient way.</p>	<p>We have asked Management whether procedures are established for reporting security incidents.</p> <p>We have verified that procedures and routines are devised for reporting and handling of security incidents, and that the reporting is submitted to the right places in the organization; see Directions.</p> <p>We have verified that the responsibility for the handling of critical incidents is clearly delegated, and that the related routines ensure that security breaches are handled expediently, efficiently, and methodically.</p>	<p>No comments.</p>

## Information Security Aspects of Business Continuity Management

Business continuity management is to counteract interruption in the company's business activities, protect critical information assets against the impact of a major crash or disaster, as well as ensure fast recovery.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>A consistent framework has been established for the company's contingency plans to ensure that all the plans are coherent and meet all security requirements and to determine the prioritisation of tests and maintenance.</p>	<p>We have asked Management whether business continuity management has been devised for online services at Continia.</p> <p>By inspection on a test basis, we have verified</p> <ul style="list-style-type: none"> <li>• that appropriate framework for preparation of business continuity management has been established</li> <li>• that contingency plans are prepared and implemented</li> <li>• that the plans include business continuity management across the organization</li> <li>• that the plans include appropriate strategy and procedures for communication with the stakeholders of Continia .</li> <li>• that contingency plans are tested on a regular basis</li> <li>• that maintenance and reassessment of the total basis for business continuity management is undertaken on a regular basis.</li> </ul>	<p>No comments.</p>

## Compliance with the Role as Data Processor

**Principles for processing personal data:**

There is compliance with procedures and controls ensuring that collecting, processing and storing of personal data are performed in accordance with the agreement about processing personal data.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>A uniform framework is established in the form of standard contracts, Service Level Agreements, as well as Data Processor Agreements or the like, containing an outline of the basis for processing personal data.</p>	<p>We have controlled the existence of updated procedures in writing for processing personal data, and that the procedures include requirements to legal processing of personal data.</p>	<p>No comments.</p>
<p>Only the kind of processing of personal data included in directions from Data Controller is performed.</p>	<p>We have controlled that Management ensures that processing of personal data is solely performed in accordance with Directions.</p> <p>We have checked, using a sample consisting of a suitable number of processing that processing is performed according to directions.</p>	<p>No comments.</p>
<p>Management immediately informs the Data Controller, if Directions in the Data Processor's view is contrary to the General Data Protection Regulation or data protection provisions according to other EU legislation or the national legislation of the member states.</p>	<p>We have controlled that Management ensures that processing is reviewed and the existence of formalised procedures securing that processing of personal data is not performed against the EU General Data Protection Regulation or other legislation.</p> <p>We have controlled the existence of procedures for informing the Data Controller in cases when processing of personal data is deemed to be against legislation.</p> <p>We have controlled that the Data Controller was informed in cases when processing of personal data was deemed to be against legislation.</p>	<p>No comments.</p>

### Data Processing:

There is compliance with procedures and controls ensuring that personal data can be erased or returned, if an agreement is entered with the Data Controller.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>There are procedures in writing with requirements about storing and erasing of personal data in accordance with the agreement with the Data Controller.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>We have controlled that there are formalised procedures for storing and erasing of personal data in accordance with the agreement with the Data Controller.</p> <p>We have checked that the procedures are updated.</p>	No comments.
<p>According to the agreement with the Data Controller, when processing of personal data is finished, data are</p> <ul style="list-style-type: none"><li>• Returned to the Data Controller, and/or</li><li>• Erased, when erasing is not against other legislation.</li></ul>	<p>We have controlled that there are formalised procedures for handling the Data Controllers' data, when processing of personal data is finished.</p> <p>We have controlled by random check using a suitable population of finished data processing cases that conducting the agreed erasing or returning of data is documented.</p>	No comments.
<p>There are procedures in writing including demands that personal data is only stored in accordance with the agreement with the Data Controller.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>We have controlled that there are formalised procedures ensuring that storing and processing of personal data are solely undertaken according to the Data Processor Agreements.</p> <p>We have checked that the procedures are updated.</p> <p>We have controlled on sample basis, whether documentation exists that data processing is conducted in accordance with the Data Processor Agreement.</p>	No comments.

**The Data Processor's responsibility:**

There is compliance with procedures and controls ensuring that solely approved sub-processors are used, and that the data processor ensures an adequate processing by follow-up on the sub-processors' technical and organizational security measures for protection of the Data Subjects' rights as well as follow-up on the processing of personal data.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>There are procedures in writing including demands to the Data Processor in relation to use of sub-processors, including demands about Sub-processor Agreements and Directions.</p> <p>On an ongoing basis, and at least once a year, assessment is made whether the procedures need updating.</p>	<p>We have controlled that there are formalised procedures regarding the use of sub-processors, including demands about Sub-processors Agreements and Directions.</p> <p>Inspected that procedures are updated.</p>	<p>No comments.</p>
<p>The Data Processor has a list of approved Sub-processors including the following information:</p> <ul style="list-style-type: none"> <li>• Name</li> <li>• CVR.no.</li> <li>• Address</li> <li>• Outline of the processing</li> </ul> <p>For processing personal data, the Data Processor solely uses Sub-processors, who are specifically or generally approved by the Data Controller.</p>	<p>We have controlled that the Data Processor has a total and updated list of approved Sub-processors used.</p> <p>Inspected that the list as a minimum includes the required information about each Sub-processor.</p> <p>Inspected using a sample of 3 Sub-processors from the Data Processor's list, it is documented that the Sub-processors' data processing is included in the Data Processor Agreements – or in other ways approved by the Data Collector.</p>	<p>No comments.</p>
<p>The Data Processor has placed the same data protection obligations on the Sub-processors as the obligations included in the Data Processor Agreement or similar document with the Data Controller.</p>	<p>We have controlled the existence of signed Sub-processor Agreements with all Sub-processors used and included in the Data Processor's list.</p> <p>Inspected using a sample of 3 Sub-processor Agreements that the agreements include the same demands and obligations as stated in the Data Processor Agreements between the Data Controllers and the Data Processor.</p>	<p>No comments.</p>

**Assisting the Data Controller:**

Procedures and controls are complied with to ensure that the Data Processor can assist the Data Controller in handing out, correcting, deleting,, or restricting processing of personal data as well as providing information about the processing of personal data to the Data Subjects.

Continia ' Control procedures	Auditor's test of controls	Test findings
<p>Written procedures exist which include a requirement that the Data Processor must assist the Data Controller in relation to the rights of Data Subjects.</p> <p>Assessments are made on a regular basis – and at least once a year – as to whether the procedures should be updated.</p>	<p>We have controlled that formalised procedures are in place for the Data Processor's assistance to the Data Controller in relation to the rights of Data Subjects.</p> <p>Inspected that procedures are up to date.</p>	<p>No comments.</p>
<p>The Data Processor has established procedures in so far as this was agreed that enable timely assistance to the Data Controller in handing out, correcting, deleting, or restricting processing as well as providing information about the processing of personal data to Data Subjects.</p>	<p>We have controlled that the procedures in place for assisting the Data Controller include detailed procedures for:</p> <ul style="list-style-type: none"> <li>• Handing out data;</li> <li>• Correcting data;</li> <li>• Deleting data;</li> <li>• Restricting the processing of personal data;</li> <li>• Providing information about the processing of personal data to Data Subjects.</li> </ul> <p>Inspected documentation that the systems and databases used support the performance of the said relevant detailed procedures.</p>	<p>No comments.</p>

**Records of processing activities:**

There is compliance with procedures and controls ensuring that the Data Processor keeps records of processing personal data for which the Data Processor is responsible.

Continia ' control procedures	Auditor's test of controls	Test findings
<p>There are records of the processing activities for each online service activity in combination with the relevant Data Controller.</p>	<p>We have controlled documentation disclosing the existence of records of processing activities for each online service activity combined with the relevant Data Controller.</p>	<p>No comments.</p>
<p>Assessment is made on an ongoing basis – and at least once a year – that the records are updated and correct.</p>	<p>We have controlled the documentation disclosing that the records of the processing activities for each Data Controller are updated and correct.</p>	<p>No comments.</p>

Reporting breaches of personal data security to the Supervisory Authority (the Danish Data Protection Agency):

There is compliance with procedures and controls ensuring that any security breaches are managed in accordance with the entered Data Processor Agreement.

Continia ' control procedures	Auditor's test of controls	Test findings
There are procedures in writing - updated at least once a year - describing how to manage personal data security breaches, including timely communication to the Data Controller.	We have controlled the existence of updated procedures in writing regarding managing personal data security breaches, including description of timely communication to the Data Controller.	No comments.
The Data Processor ensures recording of all personal data security breaches.	We have controlled documentation disclosing that all personal data security breaches are recorded at the Data Processor.	No comments.
Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	We have controlled documentation displaying that Management has ensured that all personal data security breaches are timely and sufficiently communicated to the Data Controller, including personal data security breaches happened at Data Processors used as subcontractors.	No comments.