Penneo dokumentnøgle: LSK2A-Y4PAA-G6F3T-DZSA3-AMEYU-SGGO0

Assurance report

Complea A/S

ISAE 3402 type 2 assurance report on IT general controls for
the period 1 January 2023 to 31 December 2023 related to hosting services

March 2024

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tlf. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: Complea A/S' statement

The accompanying description has been prepared for customers who have used Complea A/S' hosting services, and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Complea A/S is using subservice organisations GlobalConnect A/S and Norlys A/S. This assurance report is prepared in accordance with the carve-out method and Complea A/S' description does not include control objectives and controls within GlobalConnect A/S and Norlys A/S. Certain control objectives in the description can only be achieved, if the subsupplier's controls, assumed in the design of our controls, are suitably designed and operationally effective. The description does not include control activities performed by subsuppliers.

Some of the control areas, stated in Complea A/S' description in Section 3 of IT general controls, can only be achieved if the complementary controls with the customers are suitably designed and operationally effective with Complea A/S' controls. This assurance report does not include the appropriateness of the design and functionality of these complementary controls.

Complea A/S confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Complea A/S' hosting services processing of customer transactions throughout the period 1 January 2023 to 31 December 2023. The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:

- The type of services provided
- The procedures within both information technology and manual systems, used to manage IT general controls
- Relevant control objectives and controls designed to achieve these objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary, to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by us alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

(ii) Contains relevant information about changes in the IT general controls, performed during the period 1 January 2023 to 31 December 2023

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in their own particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period 1 January 2023 to 31 December 2023 if relevant controls with the subsupplier were operationally effective and the customers have performed the complementary controls, assumed in the design of Complea A/S' controls during the entire period from 1 January 2023 to 31 December 2023.

The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

(ii) The identified controls would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved

(iii) The controls were used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, during the period from 1 January 2023 to 31 December 2023

Nørresundby, 14 March 2024
Complea A/S

Morten Hovaldt
CEO

Section 2: Independent service auditor's assurance report on the description of controls, their design and operational effectiveness

To Complea A/S, their customers and their auditors.

Scope

We have been engaged to report on a) Complea A/S' description in Section 3 of its system for delivery of Complea A/S' services in accordance with the data processing agreement with customers as data controllers throughout the period 1 January 2023 to 31 December 2023 and about b+c) the design and operational effectiveness of controls related to the control objectives stated in the description. Complea A/S is using subservice organisations GlobalConnect A/S and Norlys A/S. This assurance report is prepared in accordance with the carve-out method and Complea A/S' description does not include control objectives and controls within GlobalConnect A/S and Norlys A/S. Certain control objectives in the description can only be achieved if the subsupplier's controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subsuppliers. Some of the control objectives stated in Complea A/S' description in Section 3 of IT general controls, can only be achieved if the complementary controls with the customers have been appropriately designed and works effectively with the controls with Complea A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Complea A/S' responsibility

Complea A/S is responsible for preparing the description in Section 3, and accompanying statement in Section 1, including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Complea A/S is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark. Grant Thornton applies International Standard on Quality Management 1, ISQM 1, requiring that we maintain a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Auditor's responsibility

Our responsibility is to express an opinion on Complea A/S' description in Section 1, as well as on the design and operation of the controls 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 International Auditing and Assurance Standards Board. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively. An assurance engagement to report on the description, design, and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls.

The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation in Section 1.

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

Limitations of controls at a service organisation

Complea A/S' description in Section 3, 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 systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

Opinion

Our opinion has been formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in Complea A/S' statement in Section 1 and based on this, it is our opinion that:

(a) The description of the IT general controls, as they were designed and implemented throughout the period 1 January 2023 to 31 December 2023, is fair in all material respects.
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 January 2023 to 31 December 2023 in all material respects, if controls with subsuppliers were operationally effective and if the customers have designed and implemented the complementary controls assumed in the design of Complea A/S' controls throughout the period 1 January 2023 to 31 December 2023.
(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 1 January 2023 to 31 December 2023.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main Section (Section 4) including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used Complea A/S and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 14 March 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Description of Complea A/S' services in connection with operating of hosting services, and related IT general controls

Description of Complea A/S in connection with supply of hosting services

In the following, Compleas services to customers is described, which are covered by the IT general controls that the declaration deals with. The declaration covers general process and system procedures at Complea A/S. Processes and procedures that are individually agreed upon with the customers of Complea, are not covered by the declaration. Assessment of any customer-specific processes and system setups will appear in specific statement to customers.

Controls in application systems are not included in this declaration.

Complea is a modern and innovative business, which was founded in 2010 and has 50 employees. The headquarter is located in Nørresundby and has a branch office in Frederikshavn. All solutions can be offered as hosting through Compleas own datacentre. This means that Complea can take over all or parts of the customers' IT solution. Complea oversees and backs up the customers' data 24/7/365, so the customers can focus on their core business.

Complea serves customers all over Denmark and offers support for the customers' international branches. All solutions are based on Complea's core values (DNA): Pride, accountability, openness, and flexibility.

Complea's short-term and long-term strategy is based in the established vision and mission. The strategy branches out through the organisation, which ensures that all employees are working towards the same goal.

Vision: Complea must be the market-leading partner in value-creating IT and digitization solutions based on human values... we are the ones being watched on the marked!

Mission: Complea's dedicated employees advise, deliver and service value adding IT solutions, that fulfils the expectations of private and public companies for technology and efficiency.

Complea provides support and IT operations so the customers' employees can always work safely and efficiently, which ensures that they can focus 100% on their core business.

Complea has its own Datacentre, which is built according to best practice and delivers a hosting service with high flexibility and stability. The service can be tailored to the customers' needs and requirements. This means that Complea can deliver a complete IT-platform with corresponding support in their own datacentre. Alternatively, Complea can also deliver a complete IT-platform onsite at the customer or through Microsoft Azure, if desired. In collaboration with the customer, a solution that gives most value to the customer is found, as it will always be an individual assessment.

IT general controls at Complea A/S

In the following, IT general controls, related to Complea's services to customers are described.

Use of subcontractors

Complea uses the subcontractor GlobalConnect and Norlys in connection with delivery of network connections.

Risk control

Complea has developed fixed procedures for risk assessment of the business and datacentre. This is to ensure that all risks are minimized to an acceptable level, so Complea can maintain normal operations in the event of risks occurring.

A periodic evaluation of the risk analysis is carried out as well as an annual review with subsequent approval by the management.

Based on the risk assessment and ISO 27002:2013, Complea has selected main areas and control targets for managing IT security, which are described in more detail below:

Organisation of IT security

The organization of IT security is based on Complea's IT security policy and is based on ISO 27002:2013 which entails the following main areas:

5	Information security policies	12	Operations security
6	Organisation of information security	13	Communications security
7	Human resource security	14	Acquisition, development, and maintenance of systems
8	Asset Management	15	Supplier relationships
9	Access control	16	Information security incident management
10	Cryptography	17	Information security aspects business continuity management
11	Physical and environmental security	18	Compliance

Organization of IT security within the individual area is described below. Control targets and controls Complea has chosen, are furthermore stated in the overview in Section 4.

Information security policies

The developed IT security policy ensures that all employees understand and comply with the established requirements and framework for IT security within Complea. At minimum a yearly review of the IT security policy is carried out.

The IT security policy is based on the fact that Complea wants to be a strong partner and ensure the delivery of stable and secure products.

IT Hardware

Controls are carried out, to ensure that all delivered data-carrying devices adheres to the IT security policy. Likewise, monitoring of all hardware are carried out to ensure that non unnotarized software are installed.

Internet, e-mail, and telephone

When onboarding new employees at Complea, they are made aware of the IT security policy, as written in the employee handbook. The employee handbook is always available to all employees. If changes are made to the employee handbook, all members of staff are informed of the changes.

Data

In the IT security policy, guidelines for how data is to be processed, is available. Correspondingly, controls are carried out to ensure that these guidelines are being followed.

Video surveillance

Video surveillance has been set up at all Complea's locations. Fixed procedures have been drawn up for storage and access to the recordings. The recordings are automatically deleted after the prescribed time periods in the IT security policy.

Organisation of information security

Complea has a standard procedure for the purpose of establishment and hiring of new employees. Correspondingly fixed controls are developed ensuring that the procedures are being complied with, and that the organizational chart is regularly updated in connection with changes in the staff.

Internal organization

IT security committee
Through knowledge sharing and further education, Complea ensures that all employees live up to the role they are intended for, and that all procedures of the IT security policy is complied with. It ensures that security matters are escalated and dealt with in accordance with the IT security policy. This is necessary, as the most important task at Complea is to secure the customers' data and organizational equipment, which also protects the business.

The strategy is evaluated yearly as the future strategy will be defined, so Complea keep evolving the business and strengthen the market position.

Internal organization mobile equipment and remote workplaces

In the IT security policy, there is a rule set regarding the use of mobile equipment and remote workplaces, which all employees must follow. This rule set will be reviewed with all new employees in relation to employment.

Surveillance is set up throughout all Compleas network in which an alarm will sound in relation to inappropriate behaviour. The IT security policy prescribes that passwords are personal and only the employee must know the password. Furthermore, security is set up, which ensures that only authorised employees have access to the systems. This is ensured through required password and screen saver in the IT security policy.

Human resource security

Human resource security requires measures to reduce the risk of human error as well as abuse and suchlike behaviour. A fixed procedure is developed before, during and after employment in Complea.

Prior to employment
There is a fixed procedure for the processing of applications, which ensures that all delivered documentation from applicant is being processed according to law.

Terms and conditions of employment
Terms of employment are described in the employment contract with the individual employee. The employee handbook will simultaneously be handed over to the employee and reviewed during the first days of employment. It is the employee's responsibility to keep updated with the employee handbook. Notice is given in the event of changes.

During employment
A criminal record of all employees at Complea is requested annually.

Management responsibility
Every employee has a direct manager in their department, who ensures that the employee's tasks and system access is equivalent to the employee's competencies and employment basis. Likewise, the immediate manager is responsible for the employee's well-being and that the employee is given the necessary information.

Awareness of, education and training in information security
There is a fixed procedure for education and training in information security. In addition, all employees are regularly informed and updated on the subject, among other things via awareness training for IT security continuously throughout the year.

Termination or change of employment
Upon termination of employment all employee data on the Complea network will be deleted with the exception of schedule for control checks, which are used to ensure that all assets are returned, and all accesses are being deactivated and deleted.

Asset management

The information security policy includes all assets, which supports Complea's business areas and organization. These include data, systems, physical assets as well as technical supplies, which supports IT-applications.

Surveillance is set up on all servers and clients, so controls can be carried out, ensuring that the IT security policy is being followed.

There is a fixed procedure in relation to the issuing of passwords and access cards to Complea's locations.

Trade agreements with customers

Complea has automatic surveillance of servers, storage, network etc. The customer can always get support 24/7/365.

Continuous testing of backup is carried out, which validates the data that Complea has backed up, while at the same time it can be recreated, if needed. A fixed procedure for security updates of the customer's servers is set in place.

In connection with start-up of new customers, a data processing agreement in accordance with the General Data Protection Regulation is delivered. A fixed procedure is in place to ensure that this agreement is sent and delivered with a signature.

Accepted use of assets
Guidelines for accepted use of assets are described in the employee handbook.

Return of assets
In accordance with the procedure for termination of employment, return of assets are secured.

New customer in the hosting centre

Complea has established a fixed procedure for the association of customers in the hosting centre. Furthermore, there is a fixed procedure for set-up and surveillance of backup. This secures a standardised set-up, in which there is a clear procedure for establishing new customers in hosting.

Data access

All customer inquiries are registered in Complea's ticket system, in which it is possible to follow correspondence between the assigned technician and the customer. This also makes it possible to control the case proceedings subsequently.

A fixed procedure is established in case of changes in the hosting centre. All changes are documented by the authorised employee at Complea and approved by the technical director.

Media handling

Management of removable media
Since Complea has the overall responsibility for relocating data, Complea ensures that no accidental data leak can occur with media in transit.

Disposal of media
A fixed procedure for destruction of all data-bearing media is established, ensuring that it is done correctly, as well as the necessary documentation is made in relation to media disposal.

Physical media in transit
Complea oversees all transportation of data-bearing hardware at existing or new customers.

Access control

Access control requires secure access to systems and data. Systems and data, including basic technical programs, are secured against unauthorized or accidental access. Access is granted, based on a work-related need, and considering an effective separation of functions.

Access control is handled through Complea's domain, which ensures that all employees adhere to the IT-security policy on passwords. Furthermore, employees who logon through remote access is registered. All remote access occurs through two factor authentication.

Business requirements of access control

Access control policy
A fixed procedure for access control in accordance with the IT-security policy is established. This procedure is reassessed continuously and in connection with changes in the staff.

User access management
The customer's user access is administered by Complea, based on a written inquiry from the customer's contact person.

Control of system access

A fixed procedure for access control is established. If there is a desire for extended access, this must be approved by the immediate manager. A limited number of employees have access to the allocation of rights.

Continuing education and knowledge sharing
The employees at Complea are considered our most important asset. Therefore, it is important to continuously ensure the employees skills, education, and certification. On an ongoing basis, internal knowledge sharing is held, to ensure that all employees are up to date with the security requirements of Complea, just as the employees attend further training throughout their employment.

User access management

Customer's inquiries are registered in Complea's ticket system, in which the customer's contact person are set up. This helps to ensure that the customer's inquiries are always approved by the customer's contact person before the task is carried out.

User registration and de-registration
It is the customer's contact person who is responsible for sending the written request to Complea in connection with the request to create a new user. Likewise, it is also the contact person who makes inquiries if a user access needs to be removed. Complea's user access to the customer's systems and data are decided by the customer. An internal procedure for granting of rights to Complea's employees is established.

User access provisioning
A fixed procedure for granting of access to each individual employee is established. Continuous revision of granted access is carried out. There is a limited number of employees who can grant access.

Management of privileged access right
It is only the management at Complea who can grant privileged access rights.

Review of use access rights
Security is the key word at Complea and because of that, an access summery which provides an overview of granted access of each employee, is made. A continuous revision of these accesses is carried out.

Removal or adjustment of access rights
The users' access rights are revised continuously and are adjusted or removed if necessary.

User responsibilities

Use of secret authentication information
Complea's IT-security policy describes that the employees' password is personal and may not be shared with others.

System and application access control

Secure logon procedures
A two-factor authentication is established for when work is carried out, outside of Complea's own network. The opportunity for remote access must be approved by the nearest department manager before access is granted.

Password management system
A GPO is established on Compleas network, which ensures that all users who are signed up to Complea's domain adheres to the prescribed guidelines for password. In connection with up linking to customer systems, it is registered which user logs on.

Cryptography

Policy on the use of cryptographic controls
Complea is always using encryption to protect data and connections.

Key management
Complea is responsible for the management of encryption keys.

Physical security and environmental security

Physical security and environmental security entails requirements and safety measures of buildings, supplies and installations relevant to Complea.

Secure areas

Complea has an access summery that outlines which locations each employee has access to. The summery is continuously revised.

Physical security perimeter

The head office is fenced of, and the main entrance is the only one which can be opened from the outside without access card.

Complea's own hosting centre, which was built in 2017, is also fenced off and only authorized personnel have access to the building. This access is reviewed yearly.

Video surveillance and anti-theft alarms are installed. The hosting centre is constructed of non-combustible material (floor, ceiling etc.). In relation to the construction there has been close dialogue with the fire authorities to ensure that the building is sufficiently secured against outbreak of fire.

Physical entry controls

An anti-theft alarm is installed on all Complea's locations and video surveillance is set up both indoors and outdoors. Deactivation of the alarm is being logged.

Access control is set up on all doors at all Complea's locations and when an employee is using their access card, it is registered when and which door the employee is using. This also applies if a door is used, which the employee does not have access to.

Securing offices, rooms, and facilities

*Hosting centre***:** The main entrance is always locked and can only be accessed by an employees with an access card. External persons (supplier or customer) can only gain access accompanied by an authorized Complea employee.

Monitoring has been set up regarding power cuts, temperature, fire, water, and humidity.

The datacentre has a high degree of redundancy and is constructed based on best practices. A minimum of one yearly test of the diesel generators are carried out where the main power is switched off in the hosting centre, resulting in the full operation being operated on a diesel generator. Correspondingly, a yearly control check of the diesel generators is carried out by the supplier, just like testing of the water-cooling system, the air filter, the ventilation, bilge pump and fire extinguisher are carried out. A fixed procedure for these tests is prescribed.

Hosting subcontractor

A fixed procedure for acquisition of yearly ISAE 3402-II declaration from the subcontractor to the hosting centre, is established. These are reviewed and approved by management.

Protection against external and environmental threats

An action plan is established in Complea's risk analysis for management of external and environmental threats. Furthermore, Complea has established various measures to reduce the likelihood of being hit by external and environmental threats.

Equipment

Equipment sitting and protection

All locations of Complea are secured with an alarm, video surveillance and access control. Likewise, server rooms are locked and can only be accessed by persons with special access.

Supporting utilities (security of supply)

A diesel generator with an automatic switch relay in the main panel is set up. The most important installations are protected by an UPS facility.

Cabling security
Cabling is set up according to best practice, both introduction and cabling into the hosting centre itself.

Securing of equipment and assets off-premises
Complea is sending data from the hosting centre to a fire-proof room in the datacentre just as an off-site backup is also sent to a secondary location.

Secure disposal or re-use of equipment
All data-bearing equipment (USB, CD/DVD, hard discs etcetera.) are destroyed before disposal to ensure that data is not accessible. If discs are disposed of, they are physically destroyed before they are handed in at an authorised recycling site. If a hard disc is recycled, an authorised wipe software is used to ensure that contents on the hard disc cannot be restored.

Operations security

Management of operations includes requirements for stability, surveillance, and security in connection with the settlement of IT production. Documentation of operational processes, operational performance, equipment, and systems has been established to a sufficient extent, to enable efficient operational performance as well as quick and effective remediation of any operational problems.

Equipment logged onto Complea's network is continuously scanned. Continuous checks are carried out to ensure that the IT security policy is complied with.

Operational procedures and responsibilities

Documented operating procedures
A fixed procedure for changes in the hosting centre is established. All changes are documented and approved by the technical director. Furthermore, there is surveillance on all essential equipment in hosting, and an alarm is sent out if unwanted events happen.

Change management
Changes are carried out only when these have been discussed, prioritised, and approved by management as well as tested under the best possible conditions. A timeslot for when changes can be made is established by agreement between Complea and the customer.

Capacity management
Complea has set up surveillance, which notifies if scaling up is required for reasons of electronic space, answer times etcetera on both internal and external systems.

Patching of systems
Complea is responsible that all relevant updates are installed such as patches, fixes, and service packs. This ensures that patching of systems is implemented and controlled so the systems are secured against downtime and unauthorised access.

Complea has a fall-back plan in connection with execution of patch management.

Protection from malware

TrendMicro, which is used for malware protection, will be installed on the employee's PC, as there is established a GPO which ensures the program is always installed, even if it is uninstalled. Furthermore, alarms are set up if threats, missing licenses, and unreliable incidents occurs.

Backup

There is surveillance in all backup jobs, which are carried out in different time intervals. If unreliable incidents occur, the operational team is informed, and action can be carried out to rectify the unintentional event.

Logging and monitoring

Event logging
All logs traced, to ensure that Complea can always trace which employee has accesses which server. Continuous control of incident logging is carried out.

Protection of log information
Log information is locked and cannot be edited.

Administrator and operator logs
Logging of administrators is carried out in connection with the normal logging.

Clock synchronization
This is ensured through domain controls.

Control of operational software

Installation of software on operational systems
Guidelines for software installation in the operation systems is described in the employee handbook. Control procedures for further control is implemented.

Communications security

Network security includes requirements of a stable network, in where the transmission of data between Complea and the customer/business partner is protected against unauthorized access and unavailability.

A fixed procedure is established for initiating customers in hosting. This is being reviewed yearly to ensure it is up to date.

Network security management

Network controls
A firewall is installed in front of all Complea's installations, as well as IP limitations (IP-filter access).

Segregation of networks
The customers are assigned their own subnet.

Information transfer

Information transfer policies and procedures
New employees with Complea are made aware of the IT-security policy, to ensure that new employees agree with the security policy.

Supplier relationships

Covers the information security requirements to manage risks associated with suppliers and outsourcing partners.

Supplier service delivery management

Monitoring and review of third-party services
An auditor's statement is requested annually from all Complea's suppliers, who supply reliable services to Complea.

Manage changes to the third-party services
If there are changes in Complea's policies or procedures, it is assessed whether there have been changes in the supplier relationship, which must be added to the risk assessment. The same will take place if the suppliers have changed their policies and services.

Information security incident management

Information security incident management includes requirements for controls, which ensures an overview of security incidents that have occurred, as well as a fast and methodological handling of security breach.

Management of information security breach and improvements

Responsibilities and procedures
The technical director is system manager on all Complea's systems and informs the organisation if changes occur in the systems that Complea uses and provides.

Reporting information security events
The ticket system is used to handling most of all customer inquiries. In the ticket system it is possible to escalate conditions where some tasks will get a bigger priority than others.

Reporting security weaknesses
The employees and external business partners are obligated to report security incidents to the immediate manager in accordance with the signed contracts, agreements, as well as the IT security policy. This ensures swift reaction to possible events.

Assessment of and decisions on information security events
Relevant employees assess the incoming tasks and solve the tasks as fast as possible after prioritising. Procedures for escalating tasks have been established.

Response to information security incidents
In case of security weaknesses, the executive board will be informed and necessary actions to reduce the incident will be taken as fast as possible. In case of bigger incidents Complea's contingency plan is activated.

Learning from information security incidents
In case of breakdown, an assessment will be carried out subsequently to avoid the same problems going forward.

Information security aspects of business continuity management

Includes requirements to the emergency management, including preparation and testing of emergency plans.

Information security continuity

Planning information security continuity
An IT emergency plan is established, in case of security breaches. All involved parties are informed about their role if an incident happens that demands the emergency plan to be activated. The emergency plan is approved by the management and is tested yearly.

Implementing information security continuity
The emergency plan is handed over to the employees who are included in the IT emergency department, to ensure the involved employees always have the IT emergency plan available.

Verify, review, and evaluate information security continuity
Yearly a desktop test is carried out on the IT emergency plan, which is verified, reviewed, and evaluated. Likewise, a fixed procedure for testing of the IT emergency plan, is in place.

Redundancies

Availability of information security processing facilities
All critical equipment in the Hosting Centre is monitored and made redundant.

Compliance

Compliance requires controls to secure against breaches on relevant IT security requirements.

Review of information security

Complea conducts an ongoing assessment if new projects/customers should be performed or rejected. Furthermore, a continuous updating of the security standards is carried out, if projects/customers are taken on that are subject to special legislation that may have an impact on the business.

Independent review of information security
A yearly evaluation of all Complea's procedures is carried out by an external IT-auditor in connection with the yearly ISAE-3402 assurance report.

Compliance with security policies and security standards
Security policies and security standards are reviewed and revised yearly, so Complea can always vouch for the highest security both internally and externally.

Examination of technical conformity
Continuous examinations are carried out to ensure that equipment, software etcetera which comply with the requirements in relation to complying with the security requirements in Complea.

Significant changes in the IT environments

No significant changes have been made to the IT application or the control environment in the period 1 January 2023 to 31 December 2023.

Complementary controls with the customers

The controls at Complea are designed so that some of the controls that are mentioned in this assurance report need to be supported with the customer's controls. The following list of complementary controls with the customers should not be considered as a complete list of controls that should be implemented by and performed at the customers.

Compleas customers are, unless otherwise agreed, responsible for:

- that there is a periodic review of the customer's own users.
- that traceability is maintained in third-party software, administered by the customer himself
- that equipment not supplied by Complea is updated.
- that internet, which is not provided by Complea, is functional.

Section 4: Control objectives, controls, and service auditor testing

Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This statement is issued according to the carve-out method and therefore does not include controls of Complea A/S' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Complea A/S' customers, are not included in this report.

Tests performed

We performed our test of controls at Complea A/S, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Complea A/S regarding controls. Inquiries have included questions on how controls are being performed.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals. The effectiveness of the controls during the audit period, is assessed by sample testing.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Test results

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with Complea A/S.

A.5 Information security policies

A.5.1 Management direction for information security

Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations

No.	*Complea A/S' control*	*Grant Thornton's test*	*Test results*
5.1.1	*Policies for information security* A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.	We have inspected that the information security policy has been approved by management and published. We have inspected that the information security policy has been reviewed and approved by the management.	No deviations noted.
5.1.2	*Review of policies for information security* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inspected documentation for regular review of the information security policy. We have inspected that the information security policy is reviewed, based on updated risk assessments to ensure that it still is suitable, adequate, and efficient.	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

No.	Complea A/S' control	Grant Thornton's test	Test results
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected an organisation chart showing the information security organisation. We have inspected that the structure is sufficient to manage the implementation and operation of information security. We have inspected the description of roles and responsibilities within the information security organisation.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.	We have inspected that conflicting duties and areas of responsibility have been defined in the organisation chart for the organisation	No deviations noted.

A.6.2 Mobile devices and teleworking
Control objective: To ensure the security of teleworking and use of mobile devices

No.	Complea A/S' control	Grant Thornton's test	Test results
6.2.1	*Mobile device policy* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected policy for securing of mobile devices. We have inspected, that technical controls for securing of mobile devices have been defined.	No deviations noted.
6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected the policy for securing of remote workspaces. We have inspected the underlaying security measures for protection of remote workspaces.	No deviations noted.

A.7 Human resource security

A.7.1 Prior to employment
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

No.	*Complea A/S' control*	*Grant Thornton's test*	*Test results*
7.1.1	*Screening* Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inspected the procedure for screening of new employees. We have, by sample test, inspected documentation that screening documentation is being obtained on new employees during the audit period.	No deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities in information security.	We have inspected the procedure for onboarding new employees. We have, by sample test, inspected documentation that new employees have been informed about their roles and responsibilities in information security.	No deviations noted.

A.7.2 During employment Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inspected the information security policy for establishing requirements for employees and contractors. We have inspected, that the management, in contracts, has required that employees and contractors must comply the information security policy.	No deviations noted.
7.2.2	*Information security awareness education and training* All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inspected procedures for ensuring adequate education and information security training (awareness training) We have inspected that activities to develop and maintain employees' security awareness have been carried out.	No deviations noted.

A.7.3 Termination and change of employment Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment or contract. We have inspected documentation that information security responsibilities and duties that remain valid after termination or change of employment have been defined and communicated.	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets
Control objective: To identify organisational assets and define appropriate protection responsibilities

No.	Complea A/S' control	Grant Thornton's test	Test results
8.1.1	*Inventory of assets* Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	We have inspected asset listings.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected list of asset ownership.	No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
8.1.3	*Acceptable use of assets* Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.	We have inspected the rules for acceptable use of assets.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inspected the procedure ensuring return of assets. We have, by sample test, inspected that assets are being returned from terminated employees.	No deviations noted.

A.9 Access control

A.9.1 Business requirements of access control
Control objective: To limit access to information and information processing facilities

No.	Complea A/S' control	Grant Thornton's test	Test results
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inspected the access control policy. We have inspected that the policy has been reviewed and approved by management.	No deviations noted.

A.9.2 User access management
Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.

No.	Complea A/S' control	Grant Thornton's test	Test results
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inspected that formalised procedures for user registration and de-registration have been established. We have, by sample test, inspected that the users' access rights have been approved. We have inspected that resigned users' access rights have been revoked.	No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services	We have inspected, that a procedure for user administration has been established. We have, by sample test, inspected that user accesses have been assigned according to the access management and control procedure. We have inquired into whether any users have changed roles or jobs during the period.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected the procedures for allocation, use and restrictions of privileged access rights. We have inspected a list of privileged users and we have inquired into whether access rights have been allocated based on a work-related need. We have inspected that privileged user accesses are personally identifiable. We have inspected, that periodical review of privileged access rights is being performed.	No deviations noted.
9.2.5	*Review of user access rights.* Asset owners are reviewing user's access rights at regular intervals	We have inspected the procedure for regular review and assessment of access rights. We have inspected, that review and assessment of access rights is being performed twice a year.	No deviations noted.
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected that resigned employees have had their access rights cancelled.	No deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
9.3.1	*Use of secret authentication information.* Users are required to follow the organisations' s practices in the use of secret authentication information.	We have inspected guidelines for use of secret passwords. We have inspected, that the implemented password policy is according to established guidelines.	No deviations noted.

A.9.4 System and application access control Control objective: To prevent unauthorised access to systems and applications			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
9.4.2	*Secure logon procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected the procedure for secure logon. We have inspected, that MFA has been established in connection with logon.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inquired that policies and procedures require quality passwords. We have inquired into whether systems for administration of access codes are configured in accordance with the requirements.	No deviations noted.

A.10 Cryptography

A.10.1 Cryptographic controls
Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

No.	*Complea A/S' control*	*Grant Thornton's test*	*Test results*
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy for the use of encryption.	No deviations noted.
10.1.2	*Key Management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic certificates, that supports the company's use of cryptographic techniques. We have inspected that cryptographic certificates are active, and that their renewal is being followed up on.	No deviations noted.

A.11 Physical and environmental security

A.11.1 Secure areas
Control objective: To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities

No.	Complea A/S' control	Grant Thornton's test	Test results
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected the procedure for physical protection of facilities and security perimeters. We have inspected relevant locations and their security perimeters to establish whether security measures have been implemented to prevent unauthorised access.	No deviations noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inspected access points to establish, whether personal access cards are used to gain access to the office. We have inspected that alarms have been installed for physical access control.	No deviations noted.
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inspected that physical security has been applied to protect offices, rooms, and facilities.	No deviations noted.

A.11.2 Equipment
Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations

No.	Complea A/S' control	Grant Thornton's test	Test results
11.2.2	*Supporting utilities (security of supply)* Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	We have inspected procedures for protection of equipment from power failure and other disruptions caused by failures in supporting utilities. We have inspected that backup power with adequate capacity is available.	No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
11.2.3	*Cabling security* Power and telecommunications cabling carrying data or supporting information services are being protected from interception	We have inspected that power- and telecommunications cabling are protected against interception and damage.	No deviations noted.
11.2.6	*Security of equipment and assets off-premises.* Security has been applied to off-site assets taking into account the different risks of working outside the organisation's premises.	We have inspected the employee handbook.	No deviations noted.
11.2.7	*Secure disposal or re-use of equipment* All items of equipment containing storage media have been verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.	We have inspected the procedure for deletion of data and software on storage media, before disposing of same.	No deviations noted.

A.12 Operations security

A.12.1 Operational procedures and responsibilities
Control objective: To ensure correct and secure operation of information processing facilities

No.	Complea A/S' control	Grant Thornton's test	Test results
12.1.1	*Documented operating procedures.* Operating procedures have been documented and made available to all users.	We have inspected that requirements for documentation and maintenance of operating procedures have been established. We have inspected that documentation for operating procedures is accessible to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure for changes in information processing facilities and systems. We have, by sample test, inspected documentation that change requests are being managed according to the established procedure.	No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
12.1.3	Capacity management The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inspected the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements. We have inspected that relevant platforms are included in the capacity requirement procedure.	No deviations noted.

A 12.2 Protection from malware Control objective: To ensure that information and information processing facilities are protected against malware			
No.	**Complea A/S' control**	**Grant Thornton's test**	**Test results**
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inspected guidelines for controls against malware. We have inspected that controls against malware have been implemented.	No deviations noted.

A.12.3 Backup Control objective: To protect against loss of data			
No.	**Complea A/S' control**	**Grant Thornton's test**	**Test results**
12.3.1	*Information backup* Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inspected documentation, that the backup procedure has been reviewed and updated during the period. We have inspected documentation of restore test being performed. We have by sample test inspected that backup has been performed as described in the procedure.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inquired into the logging of user activities. We have inspected that logging configurations contain user activities, exceptions, faults, and incidents.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inspected that log information is protected against tampering and unauthorised access.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have inspected procedures concerning logging of activities performed by system administrators and system operators.	No deviations noted.
12.4.4	*Clock synchronization* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inspected, that synchronization against a reassuring time server, has been implemented.	No deviations noted.

A.12.5 Control of operational software Control objective: To ensure the integrity of operational systems			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inspected the procedure for patching and upgrade on systems, and that is has been reviewed and updated during the period. We have inspected documentation that relevant systems are updated and patched according to specific requirements in the procedure.	No deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***Complea A/S' control***	***Grant Thornton's test***	***Test results***
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inspected the procedure regarding gathering and evaluation of technical vulnerabilities. We have inspected that Complea gathers information about technical vulnerabilities and conducts vulnerability scans.	No deviations noted.
12.6.2	*Restriction on software installation* Rules governing the installation of software by users have been established and implemented.	We have inspected documentation that general users are subject to restrictions concerning installation of software. We have inspected documentation that general users are refused if they attempt to install.	No deviations noted.

A.13 Communications security

A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

No.	Complea A/S' control	Grant Thornton's test	Test results
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inspected that requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined. We have inspected documentation for network design.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected network charts, showing segregation of development-, test-, and operations environments. We have inspected technical documentation that system environments are being segregated.	No deviations noted.

A.13.2 Information transfer
Control objective: To maintain the security of information transferred within an organisation and with any external entity

No.	Complea A/S' control	Grant Thornton's test	Test results
13.2.1	*Information transfer policies and procedures* Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.	We have inspected the procedure for managing and protection of information assets, in which transfer, and transmission of information is described.	No deviations noted.

A.15 Supplier relationships

15.2 Supplier service delivery management
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements

No.	*Complea A/S' control*	*Grant Thornton's test*	*Test results*
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inspected that the procedure for managing suppliers and supplier agreements contains requirements of yearly monitoring and review of services rendered, are according to the contract. We have inspected, that review and assessment of relevant audit reports on significant subsuppliers have been performed.	No deviations noted.
15.2.2	*Manage changes to the third-party services* Changes in supplier services, including maintenance and improvement of existing information security policies, procedures, and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have inquired about management of changes with the subcontractor, and we have inspected the documentation for handling this.	We have been informed that there have not been any changes in subcontractors during the period, wherefore it has not been possible to test the effectiveness of the control. No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements
Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

No.	*Complea A/S' control*	*Grant Thornton's test*	*Test results*
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inspected the procedure for manging security incidents. We have inspected that the procedure has been reviewed and updated during the period.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inspected guidelines for reporting of information security incidents.	We have been informed, that there have not been any information security events during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.
16.1.3	*Reporting security weaknesses* Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inspected guidelines for reporting of information security weaknesses. We have inquired into whether information security incidents have occurred during the period.	We have been informed, that there have not been any information security weaknesses during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inspected procedure for assessment of information security incidents. We have inquired into whether information security incidents have occurred during the period.	We have been informed, that there have not been any information security events during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inspected the procedure for managing information security incidents. We have inspected that the control for yearly review of incidents have been conducted. We have inquired into whether information security incidents have occurred during the period.	We have been informed, that there have not been any information security incidents during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about problem-management function which analyses information security incidents to reduce probability of recurrence. We have inspected the procedure for manging security incidents.	We have been informed, that there have not been any information security incidents during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity
Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

No.	Complea A/S' control	Grant Thornton's test	Test results
17.1.1	*Planning information security continuity* Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inspected that the contingency plan has been approved by management.	No deviations noted.
17.1.2	*Implementing information security continuity* Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	We have inspected that the contingency plan is maintained and updated as needed. We have inspected documentation that the contingency plan is accessible to relevant employees.	No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
17.1.3	*Verify review and evaluate information security continuity* The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.	We have inspected documentation that risk areas in the contingency plan have been tested during the period.	No deviations noted.

A.17.2 Redundancies Control objective: To ensure availability of information processing facilities			
No.	**Complea A/S' control**	**Grant Thornton's test**	**Test results**
17.2.1	*Availability of information security processing facilities* Information processing facilities have been implemented with redundancy sufficient to meet availability requirements.	We have inspected that redundancy has been established to ensure availability in processing facilities.	No deviations noted.

A.18.2 Information security reviews Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures			
No.	**Complea A/S' control**	**Grant Thornton's test**	**Test results**
18.2.1	*Independent review of information security* Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have inspected documentation that independent review of the information security has been performed.	No deviations noted.

No.	Complea A/S' control	Grant Thornton's test	Test results
18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inspected the list of internal controls regarding compliance with policies and standards. We have, by sample test, inspected documentation that the internal controls concerning compliance with policies and procedures, have been performed.	No deviations noted.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have, by sample test, inspected documentation that review has been performed for technical compliance with policies and standards.	No deviations noted.