Assurance report

Clever Choice ApS

ISAE 3402 type 2 assurance report on IT general controls for the period from 1 February 2023 to 31 January 2024 related to operating of ITSM & ESM solutions

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

October 2024

Table of contents

Section 1:	Clever Choice ApS' statement	1
Section 2:	Independent service auditor's assurance report on the description of controls, their design and operating effectiveness	3
Section 3:	Description of Clever Choice ApS' services in connection with operating of ITSM & ESM solutions, and related IT general controls	5
Section 4:	Control objectives, controls, and service auditor testing	12

Section 1: Clever Choice ApS' statement

The accompanying description has been prepared for customers who have used Clever Choice ApS' operating of ITSM & ESM solutions, 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.

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

Some of the control areas, stated in Clever Choice ApS' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers are suitably designed and operationally effective with Clever Choice ApS' controls. This assurance report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Clever Choice ApS confirms that:

(a) The accompanying description in Section 3 fairly presents the IT general controls related to Clever Choice ApS' operating of ITSM & ESM solutions processing of customer transactions throughout the period from 1 February 2023 to 31 January 2024. 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 from 1 February 2023 to 31 January 2024

(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 from 1 February 2023 to 31 January 2024 if relevant controls with the sub-service organisation were operationally effective and the customers have performed the complementary user entity controls, assumed in the design of Clever Choice ApS' controls during the entire period from 1 February 2023 to 31 January 2024. 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 consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 February 2023 to 31 January 2024

Roskilde, 25 October 2024
Clever Choice ApS

John Larsen
Project Director

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

To Clever Choice ApS, their customers and their auditors.

Scope

We have been engaged to report on a) Clever Choice ApS' description in Section 3 of its system for delivery of Clever Choice ApS' operating of ITSM & ESM solutions throughout the period 1 February 2023 to 31 January 2024 and about (b+c)) the design and operational effectiveness of controls related to the control objectives stated in the description.

Clever Choice ApS is using subservice organisation C-Solutions A/S. This assurance report is prepared in accordance with the carve-out method and Clever Choice ApS' description does not include control objectives and controls within C-Solutions A/S. Certain control objectives in the description can only be achieved if the subservice organisation's controls, assumed in the design of our controls, are appropriately designed and operationally effective. The description does not include control activities performed by subservice organisations.

Some of the control objectives stated in Clever Choice ApS' description in Section 3 of IT general controls, can only be achieved if the complementary user entity controls with the customers have been appropriately designed and works effectively with the controls with Clever Choice ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary user entity controls.

Clever Choice ApS' responsibility

Clever Choice ApS is responsible for preparing the description (Section 3) and accompanying statement (Section 1) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Clever Choice ApS 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 Clever Choice ApS' description (Section 3) 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 3.

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

Clever Choice ApS' 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 Clever Choice ApS' 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 from 1 February 2023 to 31 January 2024, is fair in all material respects.
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 February 2023 to 31 January 2024 in all material respects, if controls with subservice organisations were operationally effective and if the customers have designed and implemented the complementary user entity controls assumed in the design of Clever Choice ApS' controls during the period from 1 February 2023 to 31 January 2024
(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 from 1 February 2023 to 31 January 2024.

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 Clever Choice ApS 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, 25 October 2024

Grant Thornton
Godkendt Revisionspartnerselskab

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

Section 3: Description of Clever Choice ApS' services in connection with operating of ITSM & ESM solutions, and related IT general controls

IT general controls at Clever Choice

The solutions Clever Choice provides are adapted to different types of customers. The conditions for the individual customer are defined in contracts, where it is stated whether the solution is covered by an on-premises solution, or a solution hosted by Clever Choice.

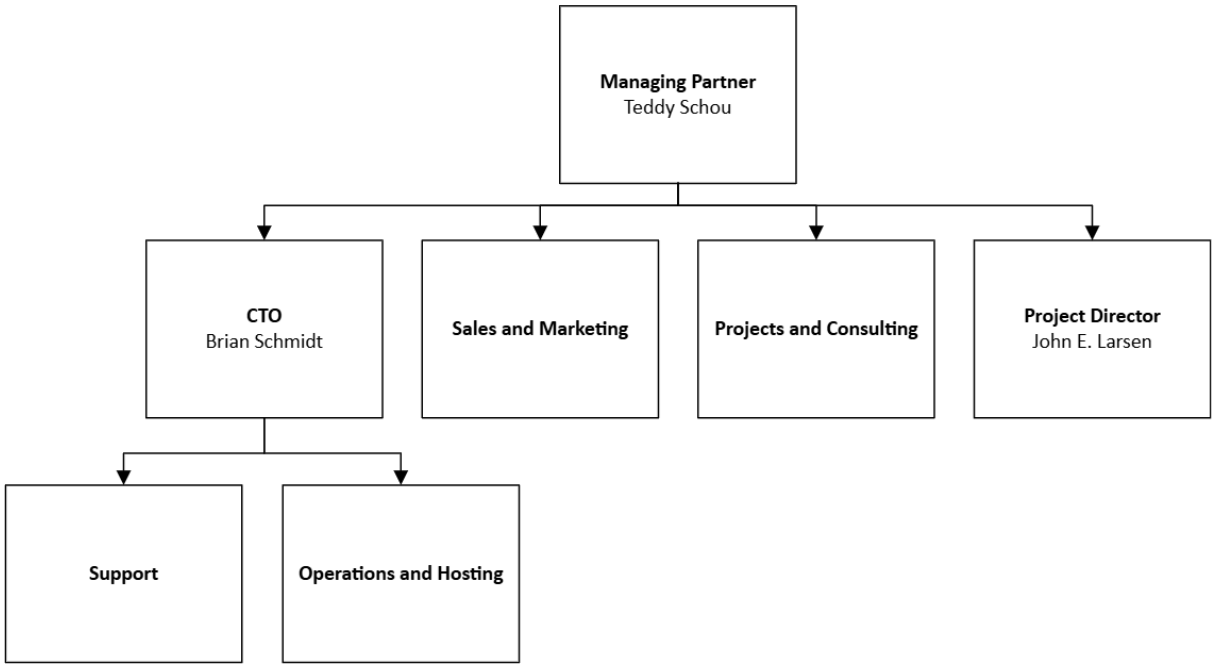
This statement covers the customers for whom Clever Choice is responsible for hosting the solution.

Clever Choice uses C-Solution as a subcontractor for all hosted solutions. C-solution is thus responsible for the physical security, hardware, network, backup, and continuity. This is covered upon receipt of an annual audit report from C-Solution.

Organisation and responsibility

Clever Choice employs approximately 15 people in sales, marketing, delivery, and support. Delivery and support are responsible for the overall delivery to customers, including implementation, hosting, and support. Support is responsible for hosted environments, including establishment, operation, monitoring, and support.

Management has the overall responsibility for IT security in Clever Choice, with the Executive Board as chief executive and ISA (IT security officer) as executive. Checks have been incorporated to ensure that management annually reviews security policy.



General information on control objectives and implemented controls

Our general description of control objectives and implemented controls:

We have defined our quality management system based on our overall goal of providing stable and secure IT operations to our customers. To do so, we have implemented policies and procedures to ensure that our deliveries are consistent and transparent.

Our IT security policy has been prepared with reference to the above and applies to all employees and to all deliveries.

Our methodology for implementing controls is defined with reference to ISO 27001/2: 2013 (Rules for managing information security), and is thus generally divided into the following control areas:

- Security policy
- Organisation of information security
- Security in relation to HR
- Asset management
- Access control
- Physical and environmental insurance
- Operational safety
- Communication security
- Supplier relations
- Security incident management
- Information security aspects of emergency management
- Compliance

The following describes our control environment in more detail for each individual area.

Information security policies

4.1 - Risk assessment

We have procedures for ongoing risk assessment of our business and especially our hosted customer environments. Thus, we can ensure that the risks associated with hosted customer environments are minimized to an acceptable level.

The risk assessment is performed periodically, as well as when changes are made to systems or the organisation that we deem relevant to reassess our general risk assessment.

The responsibility for risk assessment lies with the Information Security Officer (ISA) and must subsequently be anchored and approved by the overall management.

5.1 IT Security policy

5.1.1 IT Security policy documented

We have defined our overall methodology and approach to delivering our hosted customer environments with what it entails, in our IT security policy and associated strategic and tactical documents.

The purpose is to ensure that we have management-approved guidelines for information security in relation to our business strategy and in relation to relevant legislation.

This point is further described earlier in this description under the heading "General information about our control objectives and implemented controls."

5.1.2 Evaluation of the IT security policy

We regularly update the company's IT security policy, and at least once a year. ISA, CEO and CTO will attend the meeting on the revision of security policy.

6. Organisation of information security

6.1 Internal organisation

6.1.1 Delegation of responsibility for information security

We have a divided organisation into functional areas, which is described earlier in this document. The responsibility for information security lies with the company's overall management, which ensures that everyone in the organisation lives up to the organisation's adopted information security.

6.1.2 Functional separation

Our documentation, processes and systems help to ensure that we exclude or minimize the dependence on key people.

Functional separation is an important part of our organisation and operation, which is why we, through access controls and rights management, ensure that only authorised personnel can perform the necessary actions on systems.

6.2 Mobile equipment and remote workplaces

6.2.1 Mobile device policy

Clever Choice has a policy that forms the framework for employees' use of laptops outside the company. This ensures that our laptops are protected from access to hosted solutions.

6.2.2 Remote workplaces

Access to systems and thus potentially to customer systems and data, only takes place for authorised persons.

Access to hosted environments from the home workplace for our employees is secured via encrypted VPN connection, where the user must have a local certificate as well as a username and code to log in.

7. Security in relation to HR

7.1 Before hiring

7.1.1 Screening

We have procedures for hiring employees and for establishing collaboration with external consultants, where we ensure that we hire the right candidate in relation to background and competencies. We have role and responsibility descriptions for all key employees, so everyone is aware of their responsibilities.

7.1.2 Employment conditions

General terms of employment, including confidentiality about own and customers' conditions, are described in each employee's employment contract.

7.2 During employment

7.2.1 Management's responsibilities

In connection with employment, new employees sign a contract. The contract stipulates that the employee must comply with the policies and procedures in force at any given time. Likewise, it is clearly defined as part of the contract material what the employee's responsibilities and role are.

In connection with the use of external suppliers who have access to our systems, compliance with our policies and procedures is part of the contract. Relevant policies are part of the contract material and updates are sent electronically to the supplier. In this way, we ensure that suppliers are informed of relevant changes.

7.2.2 Awareness of education and training in information security

Awareness training is held regularly, however at least annually, to ensure that relevant employees and possibly external partners are kept up to date with our information security policy.

Employees and external parties, where it is relevant to include these under our safety guidelines, are periodically informed about our safety guidelines and when changes occur.

7.2.3 Sanctions

Internal guidelines are in place to ensure that sanctions are carried out effectively and in a timely manner. The Managing Partner and Delivery Manager are the supreme authority and the only ones who can sanction.

7.3 Termination and change of employment

7.3.1 Termination or changes in responsibilities

General terms of employment, including matters relating to termination, are described in each employee's employment contract. The overall responsibility for ensuring all controls in the resignation process lies with the employee's manager.

We have defined processes and procedures in the event of termination and changes in employment and responsibilities that ensure that access is changed / deleted and handed out equipment is returned.

8. Asset management

8.1. Liability for assets

8.1.1 List of assets

We have a procedure for registering servers and hosted customer systems in our internal system, which contains all hosted systems with associated servers.

8.1.2 Ownership of assets

Clever Choice uses security-approved vendors to host all servers. Hosting providers must provide an ISAE-3402 annually to document that they meet expected information security requirements.

8.1.3 Acceptable use of assets

In connection with the employment, employees have been informed about acceptable use of handed over assets.

8.1.4 Return of assets

Upon resignation, we have a procedure that ensures that the employee returns all relevant assets that have been handed over in connection with the employment. The procedure also ensures that the employee's rights are removed in a timely manner.

9. Access control

9.1 - Business requirements for access control

9.1.1 - Access management policies

We have a policy that ensures that only authorised personnel have access to customer systems.

9.2 - Administration of user access

9.2.1 - User creation and shutdown procedure

When hiring or changing the employee's function, there is a procedure that ensures that the employee is granted the right approved rights.

Upon resignation, we have a procedure that ensures that the employee's rights are waived so that there is no longer access to either internal systems or customer systems and customer data.

9.2.2 - Allocation of rights
Allocation of rights is covered by our normal user administration process.

9.2.3 - Control of privileged access rights
Use of passwords follows defined guidelines for complexity and renewal.

9.2.4 - Handling of confidential logon information
We inform our employees in handling confidential information, including logon information, etc.

9.2.5 - Evaluation of user access rights
Periodic checks are made that no resigned employees have rights or access to systems or data.

9.2.6 - Abolition or adjustment of access rights
We have a formal procedure for waiving and adjusting access rights.

9.3 - User Responsibility

9.3.1 - Use of confidential login information
Our information security policy stipulates that the employee's passwords must comply with minimum requirements for secure passwords.

9.4 - Control of access to systems and data

9.4.2 - Secure logon procedures
There is only access to hosted systems and customer data for relevant employees. Access can only take place either directly via the company's network in Roskilde or alternatively via VPN and secure access at other locations.

9.4.3 - Password management system

We use Active Directory to manage general user rights. Access to hosted systems and customer data are managed directly on the individual systems.

12 - Reliability

12.1 - Operational procedures and responsibilities

12.1.1 - Documented operating procedures
Through our information security policy, we have defined policies and procedures for handling IT operations. We ensure through documentation and process descriptions - and via competent employees - that all employees can start work on a system with which they do not have operational and historical experience. We operate with dual roles on selected systems, which ensures personal independence.

12.1.2 - Change management
We handle all major or significant changes via our change process, so that these are approved and documented before commissioning.

12.1.3 - Capacity management
All systems are monitored for capacity. Procedures have been developed for planning and monitoring capacity.

12.1.4 - Separation of development, testing and operating facilities
Customers' production, testing and development environments are separate and necessary access controls have been established to ensure that only authorised personnel can access systems and data.

12.2.1 – Malware
We have controls to ensure anti malware is installed on clients.

12.3.1 – Backup
We have installed daily backup that is hosted by vendor.

12.5.1 – Patch management
We have controls to ensure that patch is done correctly.

16 - Management of security incidents

16.1 Management of security incidents

Procedures and controls have been developed for handling security incidents with a focus on minimal impact on customers and avoiding compromise of customer data.

17 - Information security aspects of emergency management

Procedures and controls have been developed for efficient handling of safety incidents that require emergency management, including organisation in relation to responsibility and execution of activities.

18 - Compliance

18.2 Review of information security

The information security policy is reviewed at least once a year and relevant risk assessments, policies and procedures are updated if appropriate.

An annual IT audit is performed via an external approved inspector with a view to preparing an ISAE-3402 assurance report.

Changes in the audit period

There have been no significant changes in the audit period.

Complementary controls at customers

The controls at Clever Choice ApS are designed in such a way that some of the controls mentioned in this statement must be supplemented with controls at the customers. The following inspections are expected to be implemented and performed by and by the customers to meet the inspection objectives set out in this report. The following list of complementary controls at the customers should not be considered as an exhaustive list of controls that should be implemented by and performed at the customers (or the specific customer who is to receive the declaration).

Clever Choice customers are, unless otherwise agreed, responsible for:

- To connect to Clever Choice servers. This includes that the customers themselves are responsible for having a functioning and sufficient internet connection and possibly setting up and testing alternative internet connections in case the primary internet connection should fail.
- Regularly review the customer's user and system accounts at the application, system & database level.
- That all change requests from the customer require a formal approval of the change request. Furthermore, the customer must test the change before it can be migrated to the production environment.
- Should there be any doubt about compromised user accounts by e.g. theft of PC, it is the customers' responsibility to inform Clever Choice immediately without undue delay.
- That the customer is responsible for preparing a contingency plan for handling the customer's business in the event of major accidents or disasters.
- That the agreed level of backup covers the customer's needs
- That access to environments and data is subject to the customer's requirements for security and that there are procedures for access control at the customers
- That traceability is maintained in third-party software that the customer manages

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 Clever Choice ApS' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by Clever Choice ApS' customers, are not included in this report.

Tests performed

We performed our test of controls at Clever Choice ApS, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Clever Choice ApS 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 Clever Choice ApS.

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.	***Clever Choice ApS' 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.	We have inspected that the information security policy has been approved by management, published, and communicated to employees and relevant stakeholders. 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 inquired into the procedure 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.	Clever Choice ApS' 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 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 unauthorised or unintentional modification or misuse of the organisations' assets.	We have inspected documentation for segregation of duties. We have inspected general 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.	Clever Choice ApS' 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 relevant employees have been informed about the mobile device policy. 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 ressource 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.	*Clever Choice ApS' 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 for information security.	We have inspected the policy 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.	**Clever Choice ApS' 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 observe 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 has been carried out.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected that a formal disciplinary process has been established and communicated to employees and contractors. We have, by sample test, inspected that the disciplinary process is an integrated part of the employment contract.	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.	***Clever Choice ApS' 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. We have, by sample test, inspected that resigned employees are being informed that confidentiality agreement is still valid after termination of contract.	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.	***Clever Choice ApS' 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.	We have inspected that servers were not assigned ownership. We have inspected that ownership of servers has been assigned as a subsequent procedure. No further deviations noted

No.	Clever Choice ApS' 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 inquired dcumentation that assets are being returned from terminated employees.	We have been informed that documentation is no available showing that assets have been returned after resignation. No further 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.	Clever Choice ApS' 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.
9.1.2	*Access to network and network services.* Users are only being provided with access to the network and network services that they have been specifically authorised to use.	We have inspected that a procedure for granting access to network and network services has been established. We have inspected list of users with access to network and network services. We have inquired into whether access is based on the employees' work-related needs.	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.	***Clever Choice ApS' 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.
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign 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 once a year.	No deviations noted.

No.	Clever Choice ApS' control	Grant Thornton's test	Test results
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.	**Clever Choice ApS' control**	**Grant Thornton's test**	**Test results**
9.3.1	*Use of secret authentication information* Users are required to follow the organisations' 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. We have inspected that multifactor authentication is used for accesses.	No deviations noted.

A.9.4 System and application access control Control objective: To prevent unauthorised access to systems and applications			
No.	**Clever Choice ApS' control**	**Grant Thornton's test**	**Test results**
9.4.2	*Secure log-on 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 that systems for administration of access codes are configured in accordance with the requirements.	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.	*Clever Choice ApS' 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 updated and 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.	We have, in 5 out of 5 samples, not been provided with documentation that deployed system changes have followed the change management procedure. No further deviations noted.
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.
12.1.4	*Separation of development-, test- and operations facilities* Development testing and operational environments are separated to reduce the risks of unauthorised access or changes to the operational environment.	We have inspected technical documentation that used system environments have been separated.	No deviations noted.

A 12.2 Protection from malware Control objective: To ensure that information and information processing facilities are protected against malware			
No.	***Clever Choice ApS' 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 the policy 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.	***Clever Choice ApS' 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, by sample, inspected that backups are taken, according to the procedure. We have inspected documentation of restoretest being performed.	No deviations noted.

A.12.5 Control of operational software Control objective: To ensure the integrity of operational systems			
No.	***Clever Choice ApS' 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.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.	*Clever Choice ApS' 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 inquired into whether information security incidents are being reported through appropriate management channels.	We have been informed that no security incidents have been registered during the audit period. 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 employees have reported weaknesses or suspected weaknesses in information systems and services.	We have been informed that no security weaknesses have been reported during the audit period. 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 been managed according to the procedure.	We have been informed that no security incidents have been registered during the audit period. No deviations noted.
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 breaches. We have inquired into whether information security breaches have occurred during the period.	We have been informed that no information security breaches have been registered during the audit period. No deviations noted.

No.	Clever Choice ApS' control	Grant Thornton's test	Test results
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 breaches in order to reduce probability of recurrence. We have inquired into whether experience from information security breaches is handled.	We have been informed that no information security breaches have been registered during the audit period. 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.	Clever Choice ApS' 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 inquired about documentation showing that the contingency plan is accessible to relevant employees.	We have not been provided documentation that the contingency plan is accessible to relevant employees. No further deviations noted
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.18 Compliance

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.	*Clever Choice ApS' 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.
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 inspected documentation that the internal controls concerning compliance with policies and procedures, have been performed.	No deviations noted.