Grant Thornton

Assurance report

Clever Choice ApS

ISAE 3402 type 2 assurance report on IT general controls for the period
1 February 2022 to 31 January 2023 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

March 2023

Table of contents

Section 1: 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-premise solution, or a solution hosted by Clever Choice.

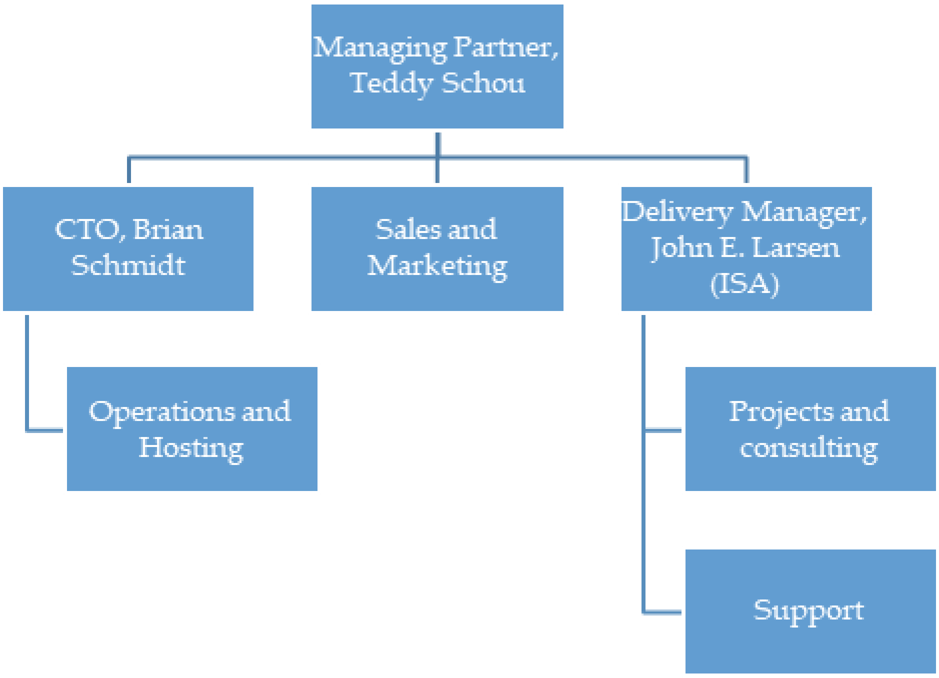
This statement covers the customers for whom Clever Choice is responsible for hosting the solution.

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.

Organization 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. The top manager is Teddy Schou, and the IT security manager is John E. Larsen



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
- Organization 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. Organization of information security

6.1 Internal Organization

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 authorized 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 authorized 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 authorized 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 authorized personnel can access systems and data.

12.2.1 – Malware

We have controls to ensue 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.

15 - Supplier relations and review.

Networks and servers are hosted and operated by external providers. Clever Choice reviews the provided assessment reports yearly.

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

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 2: 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 organisations 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.

Clever Choice ApS confirms that:

(a) The accompanying description in Section 1 fairly presents the IT general controls related to Clever Choice ApS’ operating of ITSM & ESM Solutions processing customer transactions throughout the period 1 February 2022 to 31 January 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 February 2022 to 31 January 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 February 2022 to 31 January 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 February 2022 to 31 January 2023

Roskilde, 29 March 2023
Clever Choice ApS

John Larsen
Delivery manager

Section 3: Independent service auditor's assurance report on the description of controls, their design and functionality

To Clever Choice ApS, their customers and their auditors.

Scope

We have been engaged to report on Clever Choice ApS' description in Section 1 of its system for delivery of Clever Choice ApS' services throughout the period 1 February 2022 to 31 January 2023 (the description) and on the design and operation of controls related to the control objectives stated in the description.

Clever Choice ApS is using subservice organisations 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.

Some of the control objectives stated in Clever Choice ApS' description in Section 1 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 Clever Choice ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Clever Choice ApS' responsibility

Clever Choice ApS is responsible for preparing the description (section 1) and accompanying statement (section 2) 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 behavior and ethical requirements applicable to Denmark.

Grant Thornton applies International Standard on Quality Control 1[1] and accordingly maintains 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 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.

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

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 2.

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 1, 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 2 and based on this, it is our opinion that:

(a) The description of the controls, as they were designed and implemented throughout the period 1 February 2022 to 31 January 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 February 2022 to 31 January 2023 in all material respects.
(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 February 2022 to 31 January 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 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, 29 March 2023

Grant Thornton
State Authorised Public Accountants

Kristian Randløv Lydolph
State Authorised Public Accountant

Andreas Moos
Director, CISA, CISM

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

4.1. 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.

4.2. Tests

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.
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.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

4.3. Results of tests

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 the information security policy and we have inspected documentation for management approval of the information security policy. We have inspected the procedure for periodic review of the information security policy.	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 the procedure for periodic review of the information security policy. We have inspected, that the information security policy has been reviewed, based on updated risk assessments, to ensure that it still is suitable, adequate, and effective.	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 the organisation chart. We have inspected the guidelines for information security roles and responsibilities.	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 procedures regarding granting and maintenance of segregation of duties and functions.	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 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 that procedures have been established regarding security rules in connection with the use of teleworking sites. We have inspected that secure logon procedures via two-factor authentication VPN connection have been implemented.	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 inquired into the procedure for employment of new employees and the security measures needed in the process. We have inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.	We have ascertained that the background verification check was not performed in 3 out of 4 new hires. No further 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 a selection of contracts with employees and consultants in order to determine whether the employees sign these.	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 inquired about procedure concerning establishing requirements for employees and partners. We have inspected that management has required that employees observe the IT-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 inquired about procedures to secure adequate training and education (awareness training). We have inspected documentation for activities developing and maintaining security awareness with employees.	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 sanctioning guidelines and we have inspected that the guidelines have been communicated.	We have been informed that there is no written policy covering the disciplinary process. No further 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. We have inspected documentation, that information security has been defined and communicated. We have, by sample test, inspected offboarding procedures.	We have ascertained that the offboarding procedure was not completed for 1 out of 2 terminated employees. We have however inspected that the offboarding procedure subsequently was completed for the missing employee. No further 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 that an inventory list of information security assets is available and updated.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected that ownership of information security assets are delegated.	No deviations noted.
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 that an acceptable use of asset policy has been designed and implemented.	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 inquired into the procedure for securing the return of assets delivered, and we have inspected the procedure. We have inspected a sample of returned assets.	We have ascertained that the offboarding procedure was not completed for 1 out of 2 terminated employees. We have however inspected that the offboarding procedure subsequently was completed for the missing employee. 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 that the access control policy is updated and approved.	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 authorized to use.	We have inspected that the access control policy is established covering network services. We have inspected that access to network and network services is granted based on the employees' job function and an approval from the immediate superior.	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 inquired into the procedure for creating and aborting users, and we have inspected the procedures. We have inspected a sample of documentation for user creation.	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, from a sample of users, inspected that assignment of user access rights is granted based on the job function and an approval from the immediate superior.	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
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inspected that formalized procedures for user administration and rights management have been established and that these also apply to users with privileged rights. We have inspected that authorization of privileged access rights granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior.	No deviations noted.
9.2.4	*Management of secret-authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have inspected that procedures for management of secret authentication information have been established. We have inspected that allocation of secret authentication information is controlled in accordance with the procedure.	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 that user access rights have been reviewed at regular intervals.	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, from a sample of users, inspected that removal of user access rights is performed in a timely manner upon termination or adjusted upon change of job function.	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 that a password policy is implemented. We have inspected that applications and systems enforce secure logon procedures.	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 that an access control policy is designed and updated. We have inspected that applications and systems enforce secure logon procedures.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inspected that a password policy is designed and updated. We have inspected that applications and systems enforce secure logon procedures.	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 operating procedures have been established. We have inspected that the operating procedures are accessible to all 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 that a change management policy is designed and updated. We have, from a sample of changes to systems and services, inspected that key stakeholders approve changes prior to release into production based on documented change management procedures. We have, from a sample of changes to systems and services, inspected that changes are tested based on established criteria prior to production implementation.	No 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 inquired into 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 reports.	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 unauthorized access or changes to the operational environment.	We have inspected that development, testing and operational environments are being 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, from a sample of employees' computers and servers, inspected that they are protected by antivirus software and that the software is up to date.	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 that backup copies of systems and services are made in accordance with the policy. We have inspected that restore procedures of backup copies are tested regularly and at least annually.	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 inquired about software installation guidelines on operating systems and we have, by sample test, inspected that the guidelines are followed.	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.	*Clever Choice ApS' 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 audit reports or other monitoring activities from significant suppliers is scheduled to be collected and reviewed.	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 that a formal and documented incident management procedure has been designed and updated. We have inspected that the incident management procedure includes responsibilities and has been communicated to relevant employees.	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 that a formal and documented incident management procedure has been designed and updated. We have inspected that incidents have been registered and reported through appropriate management channels in a timely manner.	No deviations noted.

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*
16.1.3	*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 observed the overview of information security events and inspected that they are reported through appropriate management channels in a timely manner.	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 the procedure for assessment, response, and evaluation of information security breaches. We have inspected that incidents have been assessed and classified	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 that a formal and documented incident management procedure has been designed and updated. We have inquired into whether information security incidents have been responded to in accordance with the documented procedures.	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 inspected that a formal and documented incident management procedure has been designed and updated. We have inquired into whether information security incidents have been analysed and resolved in accordance with the documented procedures.	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 the business continuity plan for ensuring the operations continuity in case of crashes and the like.	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 a formal and documented business continuity plan is designed and reviewed. We have inspected that underlying procedures related to the business continuity plan have been designed and reviewed.	We have ascertained that the information contingency plan has not been reviewed in 2022. 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 that a formal and documented business continuity plan is designed and updated. We have inspected that the business continuity plan has been tested to ensure the validity and effectiveness during an adverse situation.	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 observed that independent evaluation of information security has been established.	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 inquired into management's procedures for compliance with security policies and security standards. We have inspected implemented compliance controls.	No deviations noted.

PENN3O

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

John Erhardt Larsen
Underskriver 1
Serial number: 1eb52a2a-bbf4-4fe1-b007-6f6529ed6222
IP: 5.103.xxx.xxx
2023-03-29 12:25:03 UTC
MitID ✓

Andreas Moos
Underskriver 2
Serial number: eace5ed6-cfa7-4d9e-b982-120d10f47204
IP: 62.243.xxx.xxx
2023-03-29 13:21:29 UTC
MitID ✓

Kristian Lydolph
Underskriver 3
Serial number: CVR:34209936-RID:43340328
IP: 62.243.xxx.xxx
2023-03-29 13:47:17 UTC
NEM ID ✓

Penneo document key: 5ETDW-826LB-GA16Y-8CM74-UFTOO-0T0AJ