Assurance report

Lessor Group ApS

ISAE 3402 type 2 assurance report on IT general controls related to hosting services for the period 1 April 2022 to 31 March 2023

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

July 2023

Table of contents

Section 1: Description of Lessor Group ApS' services in connection with operating of hosting services, and related IT general controls

The following is a description of Lessor Group ApS' services which are included in the IT general controls of this assurance report. The report includes general processes and system setups etcetera with Lessor Group ApS. Processes and system setups etcetera, individually agreed with Lessor Group ApS' customers, are not included in this report. Assessment of customer specific processes and system setups etcetera, will be stated in specific assurance reports for customers who may have ordered such.

Controls in the application systems are not included in this report.

IT general controls at Lessor Group ApS

Introduction

In the following, a description of the IT general controls related to Lessor Group ApS' services to customers, according to the above description.

Lessor Group includes Lessor A/S and Danske Lønsystemer A/S. Throughout this document, the term Lessor Group refers to these two companies.

The object of this description is to provide information to Lessor Groups customers and their auditors concerning the requirements laid down in the international auditing standard for assurance reports on the controls at a service organisation (ISAE 3402).

Besides, the description aims to provide information about controls used for "services" with us during the period.

The description includes the control objectives and controls with Lessor Group which comprise most of our customers and are based on our standard supplies. Processes and system setups etcetera, individually agreed with customers, are not included in this report. Assessment of customer specific processes and system setups etcetera will be stated in specific assurance reports for customers who may have ordered such.

The infrastructure in scope of the description is Lessor Groups Datacenter with Linux-servers located in Allerød, Denmark. Application systems operated on the infrastructure in scope are: Danløn, LessorWorkforce, LessorLøn and LessorPortalen.

The Lessor Group has built up its control environment in accordance with ISO 27002.

Lessor and our services

The Lessor Group offers payroll and human resource management solutions in a number of countries. In Denmark and Germany, the Lessor Group ApS' primary customer group comprises companies ranging from small businesses to some of the largest Danish companies.

In this regard, we offer all relevant security measures as e.g., INERGEN® systems, cooling, redundant power sources and fibre lines and last but not least fully equipped monitoring systems.

Organisation and Responsibility

Lessor Group has a clear and transparent corporate structure and employs approximately 180 employees. The organisational structure of the Lessor Group includes the departments Administration, Finance, Development, Support and IT Operations as well as various product departments.

The employees of the Lessor Group are thus responsible for the support of our own products as well as the hosting infrastructure. The support teams handle all incoming questions. They either solve the problems or pass on the task to the Operations Department for further processing.

Thus, the Operations Department acts as second line support and monitors existing operating solutions and other tasks associated with the day-to-day management of our hosting environment.

Risk Assessment

IT Risk Analysis: Lessor Group ApS' ISO team has produced a risk analysis. On an annual basis or in case of significant changes, the group carries out a risk assessment of the assets of the Lessor Group. Both internal and external factors are taken into consideration.

The risk analysis provides an assessment of all risks identified. The risk analysis is updated on a yearly basis or in case of significant changes to ensure that the risks associated with the services provided are minimized to an acceptable level.

The responsibility for IT risk assessments lies with the CIO of the company who also approves the risk analysis.

Handling of Security Risks

Risk Management Procedure: We have implemented a scoring system for risks associated with the provision of our services.

We assess the risks which we believe we are facing point by point. We make use of a simple calculation method for this purpose: "probability %" * "impact %".

The acceptable level goes to 20 %. We continuously assess if we can reduce the risks and take initiatives to address these risks.

Security Policy

IT Security Policy

IT Security Policy Document

We have defined our quality standards system based on the general objective of providing our customers with a stable and secure hosting solution. To comply with the objectives, we have implemented policies and procedures which ensure that our supplies are uniform and transparent.

Our IT security policy is produced in accordance with ISO 27002:2013 and applies to all employees and all deliveries.

Our methodology for the implementation of controls is defined with reference to ISO 27002:2013 (guidelines for information security management) and is thus divided into the following control areas:

- Information security policies
- Organization of Information Security
- Employee safety
- Asset Management
- Conditional access
- Cryptography
- Physical security and environmental safeguards
- Operational safety
- Communication security
- Purchase, development, and maintenance of systems
- Supplier relationships
- Information security breach management
- Information security aspects related to emergency and restoration management
- Compliance

We continue to improve both policies, procedures, and operations.

Evaluation of the IT Security Policy: We update the IT security policy regularly and at least once a year. The IT security policy is approved by the CEO.

Organisation of Information Security

Internal Organisation

Delegation of Responsibility for Information Security: Our organisation is divided into different areas of responsibility. We have prepared a number of detailed responsibility and role descriptions for employees on all levels.

Confidentiality has been established for all parties involved in our business. The confidentiality is ensured via employment contracts.

Separation of Functions: Through on-going documentation and processes, we try to eliminate or minimize the dependence on key management personnel. Tasks are assigned and defined via procedures (Jira) for managing the operational services.

Contact with Special Interest Groups: The operating staff subscribes to newsletters from e.g., DK-CERT and informs itself about substantial security-related circumstances on Internet traffic.

Mobile Equipment and Teleworking

Mobile Equipment and Communication: We have made it possible for our employees to work from home via a VPN connection with two factor authentication. No equipment (portable computers etc.) must be left unattended. Portable units are protected by HDD passwords, log-in information, and HDD encryption.

Mobile devices (smart phones, tablets etc.) can be used for the synchronization of emails and the calendar. Besides the password, we have implemented no other security measures to ensure devices and user accesses.

Telecommuting: Only authorized persons are granted access to our network and thus potentially to systems and data. Our employees access the systems via telecommuting arrangements / ssh.

Human Resource Security

Prior to Employment

Screening: We have implemented procedures for the recruitment of staff and thoroughly examine the curriculum vitae of the applicant to ensure that we employ the right candidate regarding background and skills.

Conditions of Employment: The general terms of employment, e.g., confidentiality related to the customers and personal circum-stances, are specified in the employment contracts/job descriptions of all employees in which, among other things, the termination of employment and sanctions following security breaches are also described.

During Employment

Management's Responsibility: All new employees sign a contract prior to commencement of their employment. The contract provides that the employee must comply with the policies and procedures existing at any time. The contract/job description clearly defines the responsibility and role of the employee.

Awareness of and Training Activities related to Information Security: Our assets are first of all our employees. We encourage our operating staff to maintain their qualifications, educations, and certifications through training courses, lectures, and other relevant activities to ensure that the employees concerned can be kept up to date with security and become aware of new threats.

Sanctions: The general terms of employment, e.g., confidentiality related to the customers' and personal circumstances, are specified in the employment contracts of all employees in which, among other things, the termination of employment and sanctions following security breaches are also described.

Responsibility related to the Termination of Employment: When an employee terminates, a procedure will be initiated to ensure that the employee returns all relevant assets, e.g., portable devices etc. and that the access to buildings, systems and data is withdrawn. The overall responsibility to ensure all control procedures upon termination of employment lies with the CEO of the company. The documentation related to the termination of employment is available in electronic form in the human resources department.

Asset Management

Responsibility for Assets

List of Assets: Servers and network equipment including configuration are registered to be used for documentation purposes and to gain an overview of equipment etc. To secure against unauthorized access and to ensure the transparency of the structure, we have prepared some documents describing the internal network including units, naming of units, logical division of the network etc.

The documentation for equipment is updated on a regular basis and reviewed at least once a year by our operating staff.

Ownership of Assets: Central network units, servers, peripheral units, systems, and data are owned by operating staff members of the Lessor Group. The customers' data is owned by the customer's contact person.

Acceptable Use of Assets: This subject is described in the employee handbook.

Return of Assets: When an employee terminates, a procedure will be initiated to ensure that the employee returns all relevant assets and that the access to buildings, systems and data is being withdrawn. The overall responsibility to ensure all control procedures upon termination of employment lies with the CEO of the company. The documentation related to the termination of employment is available in electronic form in the human resources department.

Classification of information

We ensure appropriate protection of information commensurate witch is of importance to the organization. We make sure that all data is labeled and classified and is only processed based on documented processes.

Access Control

Access Control Requirements

Conditional Access Policies: The way the granting of access is handled is described in a policy document. The policy is part of our IT security policy.

User Access Administration

Procedures for Creation and Deletion of User Profiles: The user profiles of our customers are created solely due to the wishes of our customers. In some of the systems, the end customer himself creates his user profile without interference by the employees of the Lessor Group. Our own users are created as super users to ensure that our support teams can provide professional service.

All user profiles must be personally identifiable. The access to passwords for accounts which only are used by systems (service users) is limited to few authorized persons.

Grant of Rights: The granting of privileges is controlled in accordance with the regular user administration process. Privileges are only granted on a need-to-basis.

Handling of Confidential Login Information: Personal login information is known only by the employee and subject to a password policy to ensure the complexity.

Evaluation of User Access Rights: Periodically, i.e., once a year, we review the internal systems of the company including user profiles and access levels to ensure that the procedure related to the termination of employment is followed and that the customers' data cannot be accessed by former employees of the Lessor Group.

User Responsibility

Use of Confidential Password: The IT security policy provides that all employee passwords must be personal and that only the user knows the password. Passwords for service accounts etc. which cannot be used for logging in, and which are not changed for systemic reasons are stored in a separate system. Only six members of the Lessor Group can access this system.

Control of Access to Systems and Data

Limited Access to Data: The access for our employees is differentiated. Only systems, servers and data which are relevant to the area of work of each single employee are accessible.

System for the Administration of Passwords: All employees are subject to restrictions as regards the passwords to customer systems as well as the customers' own systems. All users have passwords which are subject to restrictions related to the creation of the passwords. Some of our systems require that the password is complex and changed regularly. In other systems, the customer himself determines the change frequency and complexity of the password.

Physical Security

Secure Areas: The physical access to the data centre of the Lessor Group in Allerød is limited to very few people from the Lessor Group who all have been provided with a key and a PIN code for the alarm system. The logical access is limited to the minimum. External partners whose task is to service the equipment in the data centre are al-ways accompanied by an employee of the Lessor Group.

Cryptography

We ensure the proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. We have policies on how we manage encryption keys and encryption techniques.

Maintenance of Equipment

Fire Safety: The Lessor Group ApS' data centre is protected against fire by two INERGEN® systems - one in each server room. Regular reviews are carried out to ensure that the INERGEN® system operates correctly. The Lessor Group has made a service contract with the supplier including two annual servicing visits. Besides, both systems are continuously monitored for operational errors.

Cooling: In the Lessor Group ApS' data centre, two refrigeration systems are installed in each server room - a free cooling system and a traditional system which also serves as a backup for the free cooling system. Regular reviews are carried out to ensure that all refrigeration systems operate correctly. The Lessor Group has made a service contract with the supplier including four annual servicing visits. Besides, all refrigeration systems are continuously monitored for operational errors.

Backup Power (UPS and generator): In the Lessor Group ApS' data centre, both UPS units and a standby generator are installed. There is a UPS unit in each server room and a common standby generator. Regular reviews are carried out to ensure that both the UPS units and the standby generator operate correctly. Both UPS systems are serviced once a year. The standby generator is serviced once a year by the supplier of the installation. Besides, both the UPS units and the standby generator are continuously monitored for operational errors.

Monitoring: The entrance to the data centre is equipped with an alarm system and under video surveillance. All Lessor Group hosting services including the infrastructure are monitored. The monitoring has been described and is being maintained continuously.

Safe Disposal or Reuse of Equipment: All data equipment is destroyed prior to disposal to ensure that no data is available.

Unattended User Equipment: All internal user accounts in the data centre are centrally managed. Screens are locked after 10 minutes in-activity. For all laptops, the time limit is 5 minutes. Thus, we minimize the risk of unauthorized access to confidential data.

Operational Safety

Change Management

Change management: All changes follow an implemented change management process and are documented in Jira.

Capacity Management: We have established a monitoring system for monitoring capacity constraints.

All incidents follow an implemented incident management process.

Protection against Malware

Measures against Malware: On Windows platforms, we have installed anti-virus software. On the firewall, we have installed an Intrusion Prevention System (IPS) to safeguard our systems against known malicious attacks.

Backup

Backup of data: We ensure that we will be able to recreate systems and data in an appropriate and correct manner in accordance with the agreements concluded with our customers. We have, for that purpose, developed a test to re-establish systems and data. The test is performed on a regular basis at least once a year.

Backups of our customers' data take place with us. Backup copies are saved in electronic form on a physical location other than the data centre.

Logging and Monitoring

Incident Logging: Network traffic and server logs are monitored and logged. All logged incidents are being reviewed. To be able to manage the monitoring and follow-up of incidents and to ensure that incidents are registered, prioritized, managed, and escalated, we have implemented formal incident and event management procedures. The process is documented in Jira.

Administrator and Operator Logs: The administrator logging process is performed simultaneously with the ordinary logging process.

Time Synchronization: We make use of Internet NTP servers for synchronization of all servers.

Managing Software in Operating Systems: Via our patch process we ensure that only approved and tested updates are being installed. All patching follows a patch management procedure.

Managing Technical Vulnerabilities: Safety warnings from DK-CERT, version 2 (or others) are monitored and analyzed. If relevant, they are installed on our internal systems within one month from the date of issue. Our internal solutions are subject to ongoing risk assessments.

Communication security

Network Measures: The IT security related to the system and data framework is made up by the Internet network, the remote network etc. All traffic, incoming as well as outgoing, is filtered by the firewall rules.

Ensuring Network Services: The customers access our systems via https. Data transferred from our systems to external partners are IP whitelisted and, if this is possible, sent via encrypted data protocols.

Our redundant firewall (a cluster solution) monitors all incoming traffic.

Network Division: Our network is divided into service segments to ensure independence between the offered services. Furthermore, test and production environments are divided into two segments.

Incident management

We ensure a consistent and effective approach to information security breach management, including communication of security incidents and vulnerabilities. We have policies in place to ensure that employees know how security breaches are defined, managed, and reported. This policy also instructs that employees are required to report information security weaknesses.

Business continuity management

Emergency Planning: Lessor has prepared an emergency plan for the handling of an emergency. The emergency plan is anchored in the IT risk analysis and maintained at least once a year following the performance of the analysis.

The plan and the procedures are anchored in our operating documentation and procedures.

Testing, Maintenance and Re-evaluation of Emergency Plans: The plan is tested once a year as a part of our emergency preparedness procedure to ensure that the customers, at the lowest possible level, will be affected by an emergency situation.

Redundancy: We seek to ensure that all services are redundant to make sure that we, in the shortest possible time, will be able to re-establish the production environment in a new environment in case of non-repairable errors in the production environment. We continue to focus on this area.

Compliance

Review of Information Security

Independent Evaluation of Information Security: An evaluation will be carried out by an external IT auditor when preparing the annual ISAE 3402 report.

Compliance with Security Policies and Standards: We carry out internal audits once a year in order to test if our internal policies and procedures are followed. The audits include all services and the infrastructure as well as other areas, if necessary.

Changes implemented during the Period

No significant changes have been implemented during the period.

Complementary Controls with the customers

Lessor's customers are, unless otherwise agreed, responsible for establishing connection to Lessor's servers. Furthermore, the customers of the Lessor Group are, unless otherwise agreed, responsible for:

- administration of their own user profiles
- their own Internet connection
- own data

Section 2: Lessor Group ApS' statement

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

Lessor Group ApS confirms that:

(a) The accompanying description in Section 1 fairly presents the IT general controls related to Lessor Group ApS' hosting services, processing customer transactions throughout the period 1 April 2022 to 31 March 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 April 2022 to 31 March 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 April 2022 to 31 March 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 April 2022 to 31 March 2023

Allerød, 21 July 2023
Lessor Group ApS

Henrik Møller
CEO

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

To Lessor Group ApS, their customers and their auditors.

Scope

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

Some of the control objectives stated in Lessor Group 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 Lessor Group ApS. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

Lessor Group ApS' responsibility

Lessor Group 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, Lessor Group 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 Thorntons 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 Lessor Group 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] ISQM 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

Lessor Group 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 Lessor Group 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 April 2022 to 31 March 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 April 2022 to 31 March 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 April 2022 to 31 March 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 Lessor Group 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, 21 July 2023

Grant Thornton
State Authorised Public Accountants

Kristian Randløv Lydolph
State Authorised Public Accountant

Martin Brogaard Nielsen
Partner, CISA, CIPP/E, CRISC

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.

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

Tests

We performed our test of controls at Lessor Group ApS, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at Lessor Group 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.

Results of tests

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with Lessor Group 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.	*Lessor Group 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, and then published and communicated to employees and relevant external parties.	We have inspected the information security policy and we have inspected documentation for management approval 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.	*Lessor Group 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 policies regarding granting and maintenance of segregation of duties and functions.	No deviations noted.
6.1.4	*Contact with special interest groups* Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.	We have inspected documentation regarding maintenance of rules for appropriate contact with special interest groups, security fora and professional organisations.	No deviations noted.

A.6.2 Mobile devices and teleworking Control objective: To ensure the security of teleworking and use of mobile devices			
No.	***Lessor Group 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 the policy for securing of mobile devices. We have inspected, that technical setup for securing of mobile devices has 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 implemented security measures.	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.	*Lessor Group 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 employment of new employees and the security measures needed in the process. We have, by sample test, inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.	No deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees are stating their and the organisation's responsibilities for information security.	We have, by sample test, inspected a contract with employees in order to determine whether these are signed by the employees.	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.	**Lessor Group 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 procedure for establishing requirements for employees. We have, by sample test, 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 inspected documentation for adequate training and education (awareness training).	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.	***Lessor Group 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, and enforced.	We have, by sample test, inspected employees' obligation to maintain information security in connection with termination of employment.	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.	*Lessor Group 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 record of asset ownership.	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 asset use guidelines.	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 for securing the return of assets delivered, and we have by sample test basis inspected the return of assets.	No deviations noted.

A.8.2 Classification of information Control objective: To ensure an appropriate protection of information considering the value of the information to the organisation.			
No.	***Lessor Group ApS' control***	***Grant Thornton's test***	***Test results***
8.2.1	*Classification* Information is classified in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification.	We have inspected the policy for classification of information.	No deviations noted.
8.2.2	*Labelling of information* An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inspected the procedures for labelling of data, and we have inspected, that information is labelled in accordance with the classification system.	No deviations noted.
8.2.3	*Handling of assets* Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inspected the procedures for handling of assets.	No deviations noted.

A.9 Access control

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

No.	Lessor Group 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 policy of managing access control in order to establish whether it 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 managing access to networks and network services, and we have inspected the solution.	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.	Lessor Group 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 the process for creating and aborting users.	No deviations noted.
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services	We have inspected that the procedure for user administration has been implemented. We have on a sample basis inspected documentation for creation and removal of user access.	We have observed that for 1 of 13 samples no ticket of approval was available for access creation. No further deviations noted.

No.	Lessor Group 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 a list of privileged users to establish whether the procedure has been followed.	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 the process regarding allocation of access codes to platforms.	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 process of periodic review of users and we have inspected checks for review.	We have observed that no formal review of user access rights has been performed for Danløn and LessorLøn. No further deviations noted.
9.2.6	*Removal or adjustment of access rights* Access rights of all employees' information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inspected procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected resigned employees and we have inspected whether their access rights have been cancelled.	No deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	**Lessor Group 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 the guidelines for use of secret authentication information.	We have not received documentation showing that the implemented password settings are in accordance with the password policy. No deviations noted.

A.9.4 System and application access control Control objective: To prevent unauthorised access to systems and applications			
No.	***Lessor Group ApS' control***	***Grant Thornton's test***	***Test results***
9.4.1	*Information access restriction* Access to information and application system functions has been restricted in accordance with the access control policy.	We have inspected guidelines and procedures for securing access restriction to application system functions.	No deviations noted.
9.4.2	*Secure log-on procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inspected procedure for secure logon.	No deviations noted.

A.10 Cryptography

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

No.	*Lessor Group ApS' control*	*Grant Thornton's test*	*Test results*
10.1.1	Policy on the use of cryptographic controls A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inspected the policy of using encryption, and we have inspected the implementation cryptography.	We have observed that Workforce is supported by TLS 1.0 and TLS 1.1. No further deviations noted.
10.1.2	*Key Management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inspected the policies for administering cryptographic keys, which supports the company use of cryptographic techniques. We have inspected that warning notification regarding cryptographic keys are implemented.	No deviations noted.

A.11 Physical and environmental security

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

No.	*Lessor Group ApS' control*	*Grant Thornton's test*	*Test results*
11.1.1	*Physical security perimeter* Security perimeters have been defined and used to protect areas that contain either sensitive or critical information and information.	We have inspected the procedure for physical security of facilities and security perimeters. We have inspected relevant locations and their security perimeter, in order to establish whether security measures have been implemented to prevent unauthorized access.	No deviations noted.
11.1.2	*Physical entry control* Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inspected procedures for access control to secure areas. We have inspected access list for authorized personnel.	No deviations noted.
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inspected that physical security has been applied to protect offices, rooms, and facilities. We have inspected, that an inspection on equipment, UPS installations etc. is being performed.	No deviations noted.
11.1.4	*Protection against external and environmental threats* Physical protection against natural disasters, malicious attack or accidents has been designed and applied.	We have inspected procedures for protection against external and environmental threats We have inspected documentation of security measures, to prevent threats from fire, heat and water and we have inspected relevant locations in order to make sure that fire-fighting equipment, fire-and smoke alarms, blocking of water-pipes, raised floors and alarms for testing of moisture, water etc. have been installed.	No deviations noted.

A.11.2 Equipment Control objective: To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations			
No.	***Lessor Group ApS' control***	***Grant Thornton's test***	***Test results***
11.2.2	*Supporting utilities (security of supply)* Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	We have inspected procedures for protection of equipment from power failure and other disruptions caused by failures in supporting utilities. We have inspected service reports showing that service inspections have been performed, according to the suppliers' recommendations, and that equipment is tested regularly.	No deviations noted.
11.2.3	*Cabling security* Power and telecommunications cabling carrying data or supporting information services are being protected from interception.	We have inspected the protection of selected power and telecommunications cabling in order to stablish whether the cables are protected from interception.	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.	*Lessor Group 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 documentation for operating procedures is accessible to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inspected the procedure regarding changes of information handling equipment and -systems. We have, by sample test, inspected whether a selection of changes, made on service applications have been registered, assessed, prioritized, and implemented in the production environment, according to the Change Management procedure. We have inquired about the change management procedure for IT Operations.	We have from 63 samples observed that: • 8 samples were not approved • 2 samples no segregation of duties was present We have been informed that a risk assessment is performed for all changes to systems, databases and networks but that the risk assessment is not formally documented at this moment. 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 unauthorized access or changes to the operational environment.	We have inspected the documentation for separation of development-, test- and operations facilities. We have inspected, that development, test, and production are either physically or logically 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.	***Lessor Group 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 procedures for measures against malware. We have inspected the documentation for the use of antivirus software.	No deviations noted.

A.12.3 Backup Control objective: To protect against loss of data			
No.	***Lessor Group 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 configuration of backup and we have inspected documentation for the setup. We have inspected that backup is monitored. We have inspected lists of backupfiles and we have inspected documentation for recovery test.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***Lessor Group ApS' control***	***Grant Thornton's test***	***Test results***
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inspected user activity logging. We have inspected procedures for system logging	No deviations noted.

No.	Lessor Group ApS' control	Grant Thornton's test	Test results
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inspected procedures for secure log information. We have inspected logging configurations in order to establish whether login information is protected against manipulation and unauthorized access.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have inspected procedures regarding logging of activities performed by system administrators and operators. We have inspected actions of system administrators and operators are logged and reviewed.	No deviations noted.
12.4.4	*Clock synchronization* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inspected the procedures for synchronization against a reassuring time server and we have inspected the solution.	No deviations noted.

A.12.5 Control of operational software Control objective: To ensure the integrity of operational systems			
No.	**Lessor Group 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 software installation guidelines on operating systems and we have, by sample test, inspected that the guidelines are followed.	No deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***Lessor Group ApS' control***	***Grant Thornton's test***	***Test results***
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inspected the procedure regarding gathering and evaluation of technical vulnerabilities.	No deviations noted.
12.6.2	*Restriction on software installation* Rules governing the installation of software by users have been established and implemented.	We have inspected the restriction of user executed software installations. We have inspected, that regulations for software installations are followed.	No deviations noted.

A.13 Communications security

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

No.	*Lessor Group ApS' control*	*Grant Thornton's test*	*Test results*
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inspected documentation for network design and security setups of network components.	No deviations noted.
13.1.2	*Security of network services* Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced.	We have inspected documentation for firewall components on the network. We have inspected that firewalls are updated.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inspected the guidelines for segregation of networks.	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.	*Lessor Group 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 responsibilities and procedures of information security incidents, and we have inspected documentation of the distribution of responsibilities. Further, we have inspected the procedure for the handling of information security incidents.	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 information security incidents, and we have inspected the guidelines. We have inspected that information events are reported appropriately.	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 inquired about information security weaknesses during the period.	We have been informed that there have not been any security weaknesses during the period, and therefore we have not been able to test the effectiveness of the control. No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inspected the procedure for assessment, response and evaluation of information security events.	No deviations noted.

No.	Lessor Group ApS' control	Grant Thornton's test	Test results
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inquired into information security incidents have been responded to, in accordance with the documented procedures.	We have been informed that there have not been any information security incidents during the period, wherefore wee have not been able to test the effectiveness of the control. No deviations noted.
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about problem management function which analyses information security incidents in order to reduce probability of recurrence.	We have been informed that there have not been any information security incidents during the period, wherefore we have not been able to test the effectiveness of the control. No deviations noted.

A.17 Information security aspects of business continuity management

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

No.	Lessor Group 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 contingency plan to ensure the continuation of operations in the event 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 procedures to ensure that all relevant systems are included in the contingency plan, and we have inspected that the contingency plan is properly maintained.	No deviations noted.

No.	Lessor Group ApS' control	Grant Thornton's test	Test results
17.1.3	*Verify review and evaluate information security continuity* The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.	We have inquired about test of the contingency plan.	We have been informed that the contingency plan has not been tested during the assurance period. No further 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.	Lessor Group 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 inspected management's procedures for compliance with security policies and security standards.	No deviations noted.

Section 5: Supplementary information from Lessor Group ApS

The following supplementary information has not been subject to the audit performed by Grant Thornton.

Based on Grant Thornton's identified deviations in the ISAE 3402 statement, Lessor A/S and Danske Lønsystemer A/S (hereinafter referred to as Lessor Group) have provided the following supplementary information:

Under control activity A.9.2.2.2, Grant Thornton has found the following:

"We have observed that for 1 out of 13 samples no ticket of approval was available for access creation.

To this, Lessor Group states that a new process has been developed to ensure approval of all new user access assignments. The observation was found for one user access grant during the transition period between the new and old process.

Under control activity A.9.2.5, Grant Thornton has found the following:

"We have observed that no formal review of user access rights has been performed for DanIøn and LessorLøn. No further deviations noted"

Lessor Group can initially state that this observation is about a small number of internal privileged admin users on the platform. These admin users are monitored on an ongoing basis and are cancelled the moment the employee in question no longer has a work-related need for these rights.

Under control activity A.9.3.1, Grant Thornton has found the following:

"We have not received documentation showing that the implemented password settings are in accordance with the password policy. No deviations noted."

To this, Lessor Group states that password settings are implemented but not possible to document on individual technical components.

Under control activity A.10.1.1.1, Grant Thornton has found the following:

"We have observed that Workforce is supported by TLS 1.0 and TLS 1.1. No further deviations noted."

To this, Lessor Group states that in the new audit period, Lessor Group requires TLS 1.2 by default.

Under control activity A.12.1.2, Grant Thornton has found the following:

”We have from 63 samples observed that: 8 samples were not approved and 2 samples no segregation of duties was present. We have been informed that a risk assessment is performed for all changes to systems, databases and networks but that the risk assessment is not formally documented at this moment. No further deviations noted.”

To this, Lessor Group states that all changes to our applications are approved. Some, such as the 8 mentioned above, are approved informally and thus could not be documented. The procedure will be tightened up so that the documentation requirement can be met in the future.

Under control activity A.17.1.3, Grant Thornton has found the following:

"We have been informed that the contingency plan has not been tested during the assurance."

To this, Lessor Group states that Lessor Group has tightened the process so that the contingency plan is tested annually.