



Building a safer society through compliance

v

## Assurance report

# Lessor Group

ISAE 3402 type 2 assurance report on general it-controls  
related to operation of hosted services during the period  
1 April 2021 to 31 March 2022

REVI-IT A/S | [www.revi-it.dk](http://www.revi-it.dk)

Højbro Plads 10, DK-1200 Copenhagen K

CVR: 30 98 85 31 | Tel. 33 11 81 00 | [info@revi-it.dk](mailto:info@revi-it.dk)

[www.dpo-danmark.dk](http://www.dpo-danmark.dk) | [www.revi-cert.dk](http://www.revi-cert.dk)

May 2022

## Table of contents

Section 1:	Description of Lessor Group ApS' services in connection with operating of hosting-services, and related general it-controls .....	1
Section 2:	Lessor Group ApS' statement .....	11
Section 3:	Independent service auditor's assurance report on the description of controls, their design and functionality.....	12
Section 4:	Control objectives, controls and service auditor testing.....	15

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

## Introduction

Lessor Group includes Lessor A/S and Danske Lønssystemer 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.

Controls in application systems and application development are not included in this report.

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 200 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 and Management

### 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. In order 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
- Organisation 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 circumstances, 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. In order 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 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.

## **Media Handling**

### **Managing Portable Devices**

We ensure, to the best possible extent, that the portable devices of our employees, e.g., portable computers, cell phones etc., are configured at the same security level as all other devices of the environment. We also ensure that all data equipment is updated when new security measures are finalized.

## 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 grant 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 six persons 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 always accompanied by an employee of the Lessor Group.

### 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 in order 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 inactivity. 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 analysed. 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.

### **Policies and Procedures for Data Transmission**

If possible, all data from the Lessor Group data centre is transmitted via encrypted protocols.

The communication with the users is done via email or support fora.

### **Confidentiality Agreements**

Confidentiality has been established for all parties involved in our business. through employment contracts and cooperation agreements with subcontractors and partners.

## **Supplier relationships**

### **Information Security in Relation to Supplier Relationships**

We require the same level of confidentiality from our suppliers as from our employees.

## **Managing Services from Third Parties**

### **Managing Changes of Services**

We do not hold review meetings with all suppliers but keep an ongoing contact with all of them.

## **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**

The following changes have been implemented during the period:

- Hired DevOps, Site Reliability Manager, Security Architect and Network Specialist
- Nutanix (hyperconverged infrastructure platform) migration completed. Consolidation of all physical infrastructure for SaaS solutions to HCI completed
- Nutanix Karbon/Kubernetes in operation
- Key cloak implemented for single sign on
- CrowdStrike Falcon endpoint security implemented on all laptops, and ongoing in data centre

## **Complementary Controls with the customers**

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

- administration of their own user profiles
- the 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' hosted 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 general it-controls related to Lessor Group ApS' hosted services processing customer transactions throughout the period 1 April 2021 to 31 March 2022. 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 general it-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 ourselves alone
    - Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to general it-controls
  - (ii) Contains relevant information about changes in the general it-controls, performed during the period 1 April 2021 to 31 March 2022
  - (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 2021 to 31 March 2022. 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 2021 to 31 March 2022

Allerød, 5 May 2022  
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' hosted services throughout the period 1 April 2021 to 31 March 2022, 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 general it-controls, can only be achieved if the complementary controls with the customers have been appropriately designed and work 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.

### REVI-IT A/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.

REVI-IT A/S applies International Standard on Quality Control 1<sup>1</sup> 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.

---

<sup>1</sup> ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.



## REVI-IT A/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.

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.

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' description 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 2021 to 31 March 2022, 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 2021 to 31 March 2022 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 2021 to 31 March 2022.

## 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 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, 5 May 2022

REVI-IT A/S

State authorised public accounting firm



Henrik Paaske

State Authorised Public Accountant



Christian H. Riis

Partner, CISA

## 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.

Our statement, does not apply to controls, performed at Lessor Group ApS' customers.

### Tests

We performed our test of controls at Lessor Group, 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 being monitored and controlled sufficiently and with adequate 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 REVI-IT as basis for the evaluation of the general it-controls with Lessor Group.

### 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	REVI-IT's test	Test results
5.1.1	<p><i>Policies for information security</i></p> <p>A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.</p>	<p>We have inspected the information security policy and we have inspected documentation of management approval of the information security policy.</p>	No deviations noted.
5.1.2	<p><i>Review of policies for information security</i></p> <p>The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.</p>	<p>We have inspected the procedure for periodic review of the information security policy.</p> <p>We have inspected the risk management assessment.</p> <p>We have inspected that the information security policy has been reviewed to ensure that it is still suitable, adequate, and effective.</p>	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	REVI-IT's test	Test results
6.1.1	<p><i>Information security roles and responsibilities</i></p> <p>All information security responsibilities are defined and allocated.</p>	<p>We have inspected the organisation chart.</p> <p>We have inspected the guidelines for information security roles and responsibilities.</p>	No deviations noted.
6.1.2	<p><i>Segregation of duties</i></p> <p>Conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.</p>	<p>We have inspected procedures regarding granting and maintenance of segregation of duties and functions.</p> <p>By inquiries and inspection of system data, we have investigated whether operating staff, only have access to administering rights on systems of which they are responsible, and whether developers have access to the production environments.</p>	No deviations noted.
6.1.4	<p><i>Contact with special interest groups</i></p> <p>Appropriate contacts with special interest groups or other specialist security forums and professional associations are maintained.</p>	<p>We have inspected the procedure regarding maintenance of rules for appropriate contact with special interest groups, security fora, and professional organisations.</p>	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	REVI-IT's test	Test results
6.2.1	<p><i>Mobile device policy</i></p> <p>Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.</p>	<p>We have inspected policy for securing of mobile devices.</p> <p>We have inspected, that technical controls for securing of mobile devices have been defined.</p> <p>We have – by sample test – inspected that technical controls are implemented on mobile devices.</p>	No deviations noted.
6.2.2	<p><i>Teleworking</i></p> <p>Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.</p>	We have inspected policy to secure teleworking, and we have inspected the underlying security measures for protection of remote workspaces.	No deviations noted.

## A.7 Human ressource security

### A.7.1 Prior to employment

Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered

No.	Lessor Group ApS' control	REVI-IT's test	Test results
7.1.1	<p><i>Screening</i></p> <p>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.</p>	<p>We have inquired into the procedure for employment of new employees and the security measures needed in the process.</p> <p>We have inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.</p>	<p>We have observed that the screening process has not been performed as described in the HR procedure.</p> <p>No further deviations noted.</p>
7.1.2	<p><i>Terms and conditions of employment</i></p> <p>The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security.</p>	We have inspected a selection of contracts with employees and consultants 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	REVI-IT's test	Test results
7.2.1	<p><i>Management responsibility</i></p> <p>Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.</p>	<p>We have inquired about procedure concerning establishing requirements for employees and partners.</p> <p>We have inquired into whether management has required the employees to observe the IT-security policy.</p>	No deviations noted.
7.2.2	<p><i>Information security awareness education and training</i></p> <p>All employees of the organisation and where relevant contractors, are receiving appropriate awareness training and regular updates in organisational policies and procedures as relevant for their job function.</p>	<p>We have inquired into procedures to secure adequate training and education (awareness training).</p> <p>We have inspected documentation for activities developing and maintaining security awareness with employees.</p>	No deviations noted.
7.2.3	<p><i>Disciplinary process</i></p> <p>There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.</p>	<p>We have inspected sanctioning guidelines and we have inspected that the guidelines have been communicated.</p>	<p>We have observed that no formal disciplinary process is described.</p> <p>No further deviations noted.</p>

### 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	REVI-IT's test	Test results
7.3.1	<p><i>Termination or change of employment responsibility</i></p> <p>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.</p>	<p>We have inquired into employees' and contractors' obligation to maintain information security in connection with termination of employment.</p> <p>We have inspected documentation, that information security has been defined and communicated.</p>	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	REVI-IT's test	Test results
8.1.1	<i>Inventory of assets</i> 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	<i>Ownership of assets</i> Assets maintained in the inventory are being owned.	We have inspected records of asset ownership.	No deviations noted.
8.1.3	<i>Acceptable use of assets</i> 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 inquired about asset use guidelines, and we have inspected the guidelines.	No deviations noted.
8.1.4	<i>Return of assets</i> 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.	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	REVI-IT's test	Test results
8.2.1	<p><i>Classification</i></p> <p>Information is classified in terms of legal requirements value criticality and sensitivity to unauthorised disclosure or modification.</p>	We have inspected the policy for classification of information.	No deviations noted.
8.2.2	<p><i>Labelling of information</i></p> <p>An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted by the organisation.</p>	We have inquired about 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	<p><i>Handling of assets</i></p> <p>Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the organisation.</p>	We have inquired about procedures for handling of assets, and we have inspected the procedures.	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	REVI-IT's test	Test results
9.1.1	<p><i>Access control policy</i></p> <p>An access control policy has been established, documented, and reviewed based on business and information security requirements.</p>	We have inquired into the policy of access control management in order to establish whether it is updated and approved.	No deviations noted.

9.1.2	<p><i>Access to network and network services</i></p> <p>Users are only being provided with access to the network and network services that they have been specifically authorized to use.</p>	<p>We have inquired into managing access to networks and network services, and we have inspected the solution.</p> <p>We have inspected several users, in order to establish if they only have access to approved networks and services, based on work-related requirements.</p>	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	REVI-IT's test	Test results
9.2.1	<p><i>User Registration and de-registration</i></p> <p>A formal user registration and de-registration process has been implemented to enable assignment of access rights.</p>	<p>We have inquired into the procedure for creating and terminating users and we have inspected the procedures.</p> <p>We have inspected a sample of documentation for user creation and removal of users.</p>	No deviations noted.
9.2.2	<p><i>User access provisioning</i></p> <p>A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services</p>	<p>We have inquired into whether a procedure for user administration has been established.</p> <p>We have inspected that the procedure for user administration has been implemented.</p>	No deviations noted.

No.	Lessor Group ApS' control	REVI-IT's test	Test results
9.2.3	<i>Management of privileged access rights</i> The allocation and use of privileged access rights have been restricted and controlled.	We have inquired about procedures for granting rights, use and limitation of privileged access rights.  We have inspected a sample of privileged users to establish whether the procedure has been followed.	No deviations noted.
9.2.4	<i>Management of secret-authentication information of users</i> The allocation of secret authentication information is controlled through a formal management process.	We have inspected the procedure regarding allocation of access codes to platforms.  We have, for a number of allocations inspected, that the procedure is being followed.	No deviations noted.
9.2.5	<i>Review of user access rights</i> Asset owners are reviewing user's access rights at regular intervals	We have inquired into the process of periodic review of users and we have inspected checks for review.  We have inquired into the procedure for the incorporation of rights and we have inspected the procedure.	No deviations noted.
9.2.6	<i>Removal or adjustment of access rights</i> Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights.  We have inspected a sample of terminated employees and we have inspected whether their access rights have been revoked.	No deviations noted.

### A.9.3 User responsibilities

Control objective: To make users accountable for safeguarding their authentication information

No.	Lessor Group ApS' control	REVI-IT's test	Test results
9.3.1	<i>Use of secret authentication information</i> Users are required to follow the organisation's practices in the use of secret authentication information.	We have inspected the guidelines for use of secret authentication information.	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	REVI-IT's test	Test results
9.4.1	<p><i>Information access restriction</i></p> <p>Access to information and application system functions has been restricted in accordance with the access control policy.</p>	<p>We have inspected guidelines and procedures for securing access restriction to application system functions.</p>	No deviations noted.
9.4.2	<p><i>Secure log-on procedures</i></p> <p>Access to systems and applications is controlled by a secure logon procedure.</p>	<p>We have inquired about procedure for secure log-on and we have inspected the implemented procedure.</p>	No deviations noted.
9.4.3	<p><i>Password management system</i></p> <p>Password management systems are interactive and have ensured quality passwords.</p>	<p>We have inquired whether policies and procedures require quality passwords</p> <p>We have inquired whether systems for administration of access codes are configured in accordance with the requirements.</p>	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	REVI-IT's test	Test results
10.1.1	<p>Policy on the use of cryptographic controls</p> <p>A policy for the use of cryptographic controls for protection of information has been developed and implemented.</p>	<p>We have inquired into the policy of using encryption, and we have – by sample test - inspected the use of cryptography.</p>	No deviations noted.
10.1.2	<p><i>Key Management</i></p> <p>A policy for the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.</p>	<p>We have inquired into the policies for administering cryptographic keys, that supports the company use of cryptographic techniques.</p> <p>We have inspected a sample of documentation, in order to establish whether the techniques are used as described.</p>	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	REVI-IT's test	Test results
11.1.1	<p><i>Physical security perimeter</i></p> <p>Security perimeters have been defined and used to protect areas that contain either sensitive or critical information.</p>	<p>We have inquired into the procedure for physical security of facilities and security perimeters.</p> <p>We have inquired into relevant locations and their security perimeter, in order to establish whether security measures have been implemented to prevent unauthorized access.</p>	No deviations noted.

No.	Lessor Group ApS' control	REVI-IT's test	Test results
11.1.2	<i>Physical entry control</i> Secure areas are protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	We have inquired into the procedures for access control to secure areas.  We have inspected a sample of access points in order to establish whether personal access cards are used to gain access to production facilities.	No deviations noted.
11.1.3	<i>Securing offices, rooms, and facilities</i> Physical security for offices rooms and facilities has been designed and applied.	We have – by sample test – inspected that physical security has been applied to protect offices, rooms, and facilities.  We have inspected, that an inspection of fire-fighting equipment, UPS installations etcetera, is performed.  We have inspected that a test of generators, UPS installations etcetera is performed.	No deviations noted.
11.1.4	<i>Protection against external and environmental threats</i> 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 inquired into the implementation 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 waterpipes, raised floors and alarms for testing of moisture, water etcetera 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	REVI-IT's test	Test results
11.2.1	<i>Equipment sitting and protection</i> Equipment is sited and protected to reduce the risks from environmental threats and hazards and opportunities for unauthorized access.	We have inquired into the procedure concerning sitting and protection of equipment.  We have inspected relevant locations, in order to determine whether the room is locked, and we have inspected that only employees with a work-related need has access.	No deviations noted.

No.	Lessor Group ApS' control	REVI-IT's test	Test results
11.2.2	<p><i>Supporting utilities (security of supply)</i></p> <p>Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.</p>	<p>We have inspected procedures for protection of equipment from power failure and other disruptions caused by failures in supporting utilities.</p> <p>We have inspected that backup power, UPS- installation and diesel generators, with adequate capacity is available.</p> <p>We have inspected service reports showing that service inspections have been performed, according to the suppliers' recommendations, and that equipment is tested regularly.</p>	No deviations noted.
11.2.3	<p><i>Cabling security</i></p> <p>Power and telecommunications cabling carrying data or supporting information services are being protected from interception</p>	<p>We have – by sample test - inspected the protection power- and telecommunications cabling in order to establish whether the cables are protected from interception.</p>	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	REVI-IT's test	Test results
12.1.1	<p><i>Documented operating procedures</i></p> <p>Operating procedures have been documented and made available to all users.</p>	<p>We have inquired into requirements for documentation and maintenance of operating procedures.</p> <p>We have inquired into whether documentation for operating procedures is accessible to relevant employees.</p>	No deviations noted.
12.1.2	<p><i>Change management</i></p> <p>Changes to the organisations business processes information processing facilities and systems that affect information security have been controlled.</p>	<p>We have inquired about the procedure regarding changes of information handling equipment and -systems.</p> <p>We have inquired whether a selection of changes, made on platforms and databases have been approved, tested, documented, and implemented in the production environment, according to the change management procedure.</p>	No deviations noted.
12.1.3	<p><i>Capacity management</i></p> <p>The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.</p>	<p>We have inquired into the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements.</p> <p>We have inspected that relevant platforms are included in the capacity requirement procedure.</p>	No deviations noted.
12.1.4	<p><i>Separation of development-, test- and operations facilities</i></p> <p>Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.</p>	<p>We have inquired into securing the separation of development-, test- and operations facilities.</p> <p>We have – by sample test - inspected, that development, test, and production are either physically or logically separated.</p>	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	REVI-IT's test	Test results
12.2.1	<p><i>Control against malware</i></p> <p>Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.</p>	<p>We have inquired into measures against malware.</p> <p>We have inquired about the use of antivirus software and we have inspected documentation for its use.</p>	No deviations noted.

#### A.12.3 Backup

Control objective: To protect against loss of data

No.	Lessor Group ApS' control	REVI-IT's test	Test results
12.3.1	<p><i>Information backup</i></p> <p>Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.</p>	<p>We have inquired into configuration of backup and we have inquired samples of documentation for the setup according to requirements.</p> <p>We have inquired into testing of backupfile recovery.</p>	No deviations noted.

#### A.12.4 Logging and monitoring

Control objective: To record events and generate evidence

No.	Lessor Group ApS' control	REVI-IT's test	Test results
12.4.1	<p><i>Event logging</i></p> <p>Event logs recording user activities, exceptions, faults, and information security events have been produced, kept, and regularly reviewed.</p>	<p>We have inquired into user activity logging.</p> <p>We have inspected samples of logging configurations.</p>	No deviations noted.

No.	Lessor Group ApS' control	REVI-IT's test	Test results
12.4.2	<i>Protection of log information</i> Logging facilities and log information are being protected against tampering and unauthorized access.	We have inquired about secure log information and we have inspected the solution.  We have inquired into a selection of logging configurations in order to establish whether login information is protected against manipulation and unauthorized access.	No deviations noted.
12.4.3	<i>Administrator and operator logs</i> System administrator and system operator activities have been logged, and the logs protected and regularly reviewed.	We have inquired into procedures regarding logging of activities performed by system administrators and operators.  We have inquired about logon setups on servers and database systems, in order to establish whether the actions of system administrators and operators are being logged.	No deviations noted.
12.4.4	<i>Clock synchronization</i> 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 inquired into procedures for clock synchronization 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	REVI-IT's test	Test results
12.5.1	<i>Installation of software on operational systems</i> 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 being followed.	No deviations noted.



#### A.12.6 Technical vulnerability management

Control objective: To prevent exploitation of technical vulnerabilities

No.	Lessor Group ApS' control	REVI-IT's test	Test results
12.6.1	<p><i>Management of technical vulnerabilities</i></p> <p>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.</p>	<p>We have inquired into the procedure regarding gathering and evaluation of technical vulnerabilities.</p> <p>We have inquired about penetration test and have inspected the test results.</p>	No deviations noted.
12.6.2	<p><i>Restriction on software installation</i></p> <p>Rules governing the installation of software by users have been established and implemented.</p>	We have inquired into restriction of user executed software installations.	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	REVI-IT's test	Test results
13.1.1	<p><i>Network controls</i></p> <p>Networks are managed and controlled to protect information in systems and applications.</p>	<p>We have inquired into the policy for network controls.</p> <p>We have inspected the policy for network controls.</p> <p>We have inquired into whether requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined.</p>	No deviations noted.
13.1.2	<p><i>Security of network services</i></p> <p>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.</p>	<p>We have observed that written requirements about security mechanisms, service levels and management requirements of all network services, are present.</p> <p>We have inspected a range of network components to estimate whether the components have been set up according to requirements and contractor's recommended baselines.</p>	No deviations noted.
13.1.3	<p><i>Segregation of networks</i></p> <p>Groups of information services users and information systems are segregated on networks.</p>	<p>We have inquired into the guidelines for segregation of networks.</p> <p>We have inquired into an overview of networks.</p>	No deviations noted.

### A.13.2 Information transfer

Control objective: To maintain the security of information transferred within an organisation and with any external entity

No.	Lessor Group ApS' control	REVI-IT's test	Test results
13.2.1	<p><i>Information transfer policies and procedures</i></p> <p>Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.</p>	We have inquired into data transfer policies and procedures.	No deviations noted.
13.2.2	<p><i>Agreements on information transfer</i></p> <p>Agreements address the secure transfer of business information between the organisation and external parties.</p>	<p>We have inquired into data transfer agreements.</p> <p>We have inquired into agreements with customers and other external parties, describing the requirements for safe exchange of data.</p>	No deviations noted.
13.2.4	<p><i>Confidentiality or non-disclosure agreements</i></p> <p>Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information, are identified, and documented on a regular basis.</p>	We have inquired into the procedure for establishing non-disclosure agreements. We have inspected a range of signed non-disclosure agreements to establish whether the procedure has been followed when hiring of new staff and closing of agreements with customers.	No deviations noted.

## A.15 Supplier relationships

### A.15.1 Information security in supplier relationships

Control objective: To ensure protection of the organisation's assets that are accessible by suppliers

No.	Lessor Group ApS' control	REVI-IT's test	Test results
15.1.1	<p><i>Information security policy for supplier relationships</i></p> <p>Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets have been agreed with the supplier and documented.</p>	<p>We have inquired into the procedure for closing agreements with subcontractors.</p> <p>We have inspected the information security policy for supplier relationships.</p>	No deviations noted.
15.1.2	<p><i>Addressing security within supplier agreements</i></p> <p>All relevant information security requirements are established and agreed with each supplier that may access process store communicate or provide IT infrastructure components for the company's information.</p>	<p>We have inquired into the procedure for conclusion of contract with subcontractors.</p> <p>We have inquired about samples of contracts with subcontractors.</p> <p>We have inspected a standard subcontractor contract.</p>	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	REVI-IT's test	Test results
16.1.1	<p><i>Responsibilities and procedures</i></p> <p>Management responsibilities and procedures are established to ensure a quick, effective, and orderly response to information security incidents.</p>	<p>We have inquired into the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities.</p> <p>Furthermore, we have inspected the procedure for handling information security incidents.</p>	No deviations noted.
16.1.2	<p><i>Reporting information security events</i></p> <p>Information security events are being reported through appropriate management channels as quickly as possible.</p>	We have inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines.	No deviations noted.
16.1.3	<p><i>Reporting security weaknesses</i></p> <p>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.</p>	We have inquired about information security events during the period and we have inspected these.	No deviations noted.
16.1.4	<p><i>Assessment of and decision on information security events</i></p> <p>Information security events are assessed, and it is decided if they are to be classified as information security incidents.</p>	We have inquired into the procedure for assessment, response and evaluation of information security breaches.	No deviations noted.
16.1.5	<p><i>Response to information security incidents</i></p> <p>Information security incidents are responded to in accordance with the documented procedures.</p>	We have – by sample test - inspected that information security incidents have been responded to, in accordance with the documented procedures.	No deviations noted.

No.	Lessor Group ApS' control	REVI-IT's test	Test results
16.1.6	<p><i>Learning from information security incidents</i></p> <p>Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.</p>	We have inquired about problem management function which analyses information security incidents in order to reduce probability of recurrence.	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	REVI-IT's test	Test results
17.1.1	<p><i>Planning information security continuity</i></p> <p>Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been determined.</p>	We have inquired into the preparation of a contingency plan to ensure the continuation of operations in the event of crashes and the like, and we have inspected the plan.	No deviations noted.
17.1.2	<p><i>Implementing information security continuity</i></p> <p>Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established documented implemented and maintained.</p>	We have inquired into 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	REVI-IT's test	Test results
17.1.3	<p><i>Verify review and evaluate information security continuity</i></p> <p>The established and implemented information security continuity controls are verified at regular intervals in order to ensure that they are valid and effective during adverse situations.</p>	<p>We have inquired into test of the contingency plan, and we have inspected documentation for tests performed.</p> <p>We have also inquired into reassessment of the contingency plan, and we have inspected documentation for reassessment.</p>	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

	Lessor Group ApS' control	REVI-IT's test	Test results
18.2.1	<p><i>Independent review of information security</i></p> <p>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.</p>	We have observed that independent evaluation of information security has been established.	No deviations noted.
18.2.2	<p><i>Compliance with security policies and standards</i></p> <p>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.</p>	We have inquired into management's procedures for compliance with security policies and security standards.	No deviations noted.