ISAE 3402 Type 2 report on General IT Controls regarding Lessor Group's operation of hosted services for the period 01 April 2019 to 31 March 2020

Lessor Group

May 2020

REVI-IT A/S • state authorized public accounting firm
Jens Kofods Gade 1 • DK-1268 Copenhagen K • Phone 3311 8100 • info@revi-it.dk • revi-it.dk • CVR-no. 3098 8531

Table of contents

Section 1: Lessor Group's description of the control and hosting environment

Introduction

The Lessor Group is composed of:

- Lessor A/S
- Lessor GmbH
- Danske Lønsystemer A/S
- ilohngehalt internetservices GmbH
- NORLØNN AS
- Swelönn AB

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 organization (ISAE 3402).

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

The description includes the control objectives and controls with Lessor Group, which comprise most of our customers and are based on our standard supplies. Individual customer relationships are not covered by this description.

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

Lessor Group 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's primary customer group comprises companies ranging from small businesses to some of the largest Danish companies. In the other countries in which the Lessor Group is also represented, the focus is fixed on small businesses with few employees.

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.

The Lessor Group only offers professional cloud services.

The infrastructure used to operate the following applications from Lessor Group:, is part of the scope of this ISAE 3402 Report: Danlon, Workforce, Lessor5, Portal, Swelon, Norlon and ilongehalt.

Organization and responsibility

Lessor Group has a clear and transparent corporate structure and employs approximately 150 employees. The organizational 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's 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 risk assessments lies with the CEO 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.

Information security policies

IT security policy

IT security policy document

We have defined our quality standards system on the basis of 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
- 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 organization

Delegation of responsibility for information security
Our organization 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 devices 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 with regard to 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.

Termination and change 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

Business requirements of access control

Conditional access policies

The manner in which the granting of access is handled is described in a policy document. The policy is part of our IT security policy.

User access management

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 are able to 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 responsibilities

Use of confidential password

The IT security policy provides that all employee password 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.

System and application access control

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 be complex and changed regularly. In other systems, the customer himself determines the change frequency and complexity of the password.

Physical and environmental 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.

Equipment

Fire safety

The Lessor Group's 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's 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's 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 security

Operational procedures and responsibilities

Documented operating procedures

As some tasks are performed by one employee only, we have prepared some detailed descriptions in order to ensure that we can re-establish a given service in a new environment.

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 from 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.

Protection of login information
Logs are uploaded to our own log server and protected against modification and deletion.

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.

Control of operational software

Via our patch process we ensure that only approved and tested updates are being installed. All patching follows a patch management procedure.

Technical vulnerability management
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 security management
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 white listed 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.

Information transfer
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.

Purchase, development and maintenance

Safety requirements for information systems

Analysis and specification of safety requirements
When a new system is implemented, a number of analysis and research procedures is performed in order to ensure that the system fully complies with the rules and security policies adopted by the Lessor Group.

Change management procedures
All changes follow an implemented change management process.

Our test and production environments are logically and physically separated.

Limitation of software package changes
Service packs and system specific updates which may involve changes in functionality are assessed and installed separately. Security updates are, as far as possible, implemented in all systems. In the first instance, they will be implemented only in the test environment. If the product manager accepts the updates (that is if the service works as intended after the update process), the same security updates will be implemented in the production environment.

Supplier relationships

Information security in supplier relationships
We require the same level of confidentiality from our suppliers as from our employees.

Supplier service delivery management

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

Information security incident management

Management of information security incidents and improvements

Emergency planning
Lessor Group 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

Information security reviews

Independent evaluation of information security
An evaluation will be carried out by an external IT auditor and 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.

Complementary user entity controls (CUECs)

The controls with Lessor Group, have been designed in such a way, that some of the controls mentioned in this report must be supplemented by controls at the customers. Below mentioned controls are expected to be implemented and performed at the customer, by the customer, in order to fulfil the control objectives stated in this report. Below mentioned complementary user entity controls are not to be regarded as a comprehensive listing of controls, that should be implemented and performed at the customers.

- Administration of their own user profiles in the applications supplied
- Their own Internet connection between the customer and Lessor Group
- Completeness and accuracy of own data in the applications supplied
- Regular review of assigned user rights in own user profiles in the applications supplied

Significant changes implemented during the period

No significant changes have been implemented during the period.

Section 2: Lessor Group's statement

This description has been prepared for customers who have made use of Lessor Group's hosting services, and for their auditors who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Lessor Group confirms that:

(a) The accompanying description in Section 2, fairly presents Lessor Group's hosting services related to customer transactions processed throughout the period 01 April 2019 to 31 March 2020. The criteria for this statement were that the included description:

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

- The type of services provided, when relevant
- The procedures, within both information technology and manual systems, by which transactions are initiated, recorded, processed, corrected as necessary, and transferred to the reports presented to the customers
- 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 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 considered relevant to processing and reporting customer transactions

(ii) Provides relevant details of changes in the service organisation's system throughout the period 01 April 2019 to 31 March 2020

(iii) Does not omit or distort information relevant to the scope of the described system, 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 to their particular environment

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 01 April 2019 to 31 March 2020. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period of 01 April 2019 to 31 March 2020.

Allerød, 13 May 2020

Lessor Group

Henrik Møller
CEO

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

To Lessor Group, their customers, and their auditors.

Scope

We have been engaged to report on Lessor Group's description, presented in Section 1. The description, as confirmed by the management of Lessor Group in Section 2, covers Lessor Group's operating and hosting services in the period 01 April 2019 to 31 March 2020 as well as the design and operation of the controls related to the control objectives stated in the description.

Our opinion is issued with reasonable assurance.

Lessor Group's responsibility

Lessor Group is responsible for preparing the description (Section 1) and the related statement (Section 2) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, Lessor Group is responsible for providing the services covered by the description, 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 Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

REVI-IT A/S 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.

REVI-IT A/S' responsibility

Our responsibility is to express an opinion on Lessor Group's 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.

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

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's 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 systems that each individual customer may consider important in its 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.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion were those described in Lessor Group's description in Section 2 and on the basis of this, it is our opinion that:

(a) the description of the controls, as they were designed and implemented throughout the period 01 April 2019 to 31 March 2020, is fair in all material respects
(b) the controls related to the control objectives stated in the description were suitably designed throughout the period 01 April 2019 to 31 March 2020 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 01 April 2019 to 31 March 2020.

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).

Intended users and purpose

This assurance report is intended only for customers who have used Lessor Group's services 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, 13 May 2020

REVI-IT A/S
State authorized public accounting firm

Henrik Paaske
State Authorized Public Accountant

Christian H. Riis
Director, CISA

Section 4: Control objectives, controls, tests, and related test controls

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.

Tests of the operating effectiveness of specific controls included such tests as were considered necessary in the circumstances to evaluate whether those controls, and the extend of compliance with them, are sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period from 01 April 2019 to 31 March 2020. Tests of the operating effectiveness of controls were designed to cover each of the controls listed in Section 4, which are designed to achieve the specified control objectives. In selecting particular tests of the operating effectiveness of controls REVI-IT A/S considered the nature of the controls being tested, the types and competence of available evidence, the control objectives to be achieved, and the expected efficiency and effectiveness of the test.

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

We performed our tests of controls at Lessor Group by taking the following actions:

Method	General description
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 efficient when implemented.
Observation	Observing how controls are performed.
Inquiries	Interview with appropriate personnel at Lessor Group regarding controls.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

Risk assessment and management

Risk assessment

Control objective: To ensure that the company periodically performs an analysis and assessment of the IT risk profile.

No.	Lessor Group's control	REVI-IT's test	Test results
4.1	Lessor Group's 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 risk assessments lies with the CEO of the company who also approves the risk analysis.	We have enquired about the preparation of an IT risk analysis, and we have inspected the prepared IT risk analysis. We have enquired about periodic review of the IT risk analysis, and we have inspected documentation for review during the audit period. We have enquired about the management's approval of the IT risk analysis, and we have inspected documentation for management approval.	No deviations noted.

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's control	REVI-IT'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 have been 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 to ensure that it still is suitable, adequate, and efficient.	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation

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

No.	Lessor Group's control	REVI-IT's test	Test results
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected the organization 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 organizations' assets.	We have inspected the information security frame to ensure that segregation of duties has been considered.	No deviations noted.
6.1.3	*Contact with authorities* Appropriate contacts with relevant authorities are maintained.	We have inspected the procedure for contact with authorities.	No deviations noted.

No.	Lessor Group's control	REVI-IT's test	Test results
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 the procedure for contact with special interest groups.	No deviations noted.
6.1.5	*Information security in project management* Information security is addressed in project management, regardless of the type of project.	We have inspected the procedure for project management to ensure that information security is addressed.	No deviations noted.

A.6.2 Mobile devides and teleworking

Control objective: To ensure the security of teleworking and use of mobile devices within the organisation.

No.	Lessor Group's control	REVI-IT's test	Test results
6.2.1	*Mobile device policy* A policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected the mobile device policy.	No deviations noted.
6.2.2	*Teleworking* A policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected the teleworking policy.	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's control	REVI-IT's test	Test results
7.1.1	*Screening* Background verification checks on all candidates for employment is being carried out in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inquired into the procedure for employment of new employees and the security measures needed in the process. We have inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.	No deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organization's responsibilities for information security.	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's control	REVI-IT's test	Test results
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inquired about procedure concerning establishing requirements for employees and partners. We have inquired that management has required that employees observe the IT-security policy.	No deviations noted.

No.	Lessor Group's control	REVI-IT's test	Test results
7.2.2	*Information security awareness education and training* All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inquired about procedures to secure adequate training and education (awareness training). We have inspected documentation for activities developing and maintaining security awareness with employees.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to take action against employees who have committed an information security breach.	We have inspected sanctioning guidelines and we have inspected that the guidelines have been communicated.	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's control	REVI-IT's test	Test results
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment. We have inspected documentation, that information security has been defined and communicated.	No deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets

Control objective: To identify organizational assets and define appropriate protection responsibilities.

No.	Lessor Group's control	REVI-IT'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 inquired about asset use guidelines and we have inspected the guidelines.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organizational 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 Information classification

Control objective: To ensure that the information receives an appropriate level of protection in accordance with its importance to the organisation.

No.	Lessor Group's control	REVI-IT's test	Test results
8.2.1	*Classification of information* Information is classified in terms of legal requirements value criticality and sensitivity to unauthorized disclosure or modification.	We have inquired into the policy for data classification and we have inspected the policy.	No deviations noted.
8.2.3	*Handling of assets* Procedures for handling assets have been developed and implemented in accordance with the information classification scheme adopted by the organisation.	We have inquired about asset management guidelines and we have inspected the guidelines.	No deviations noted.

A.8.3 Media handling

Control objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.

No.	Lessor Group's control	REVI-IT's test	Test results
8.3.1	*Management of removable media* Procedures have been implemented for the management of removable media in accordance with the classification scheme adopted by the organisation.	We have inquired about managing portable media and we have inspected documentation for the solution.	No deviations noted.
8.3.2	*Disposal of media* Media are being disposed of securely when no longer required using formal procedures.	We have inquired about media disposal guidelines. We have inspected that media are disposed of, according to 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's control	REVI-IT'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 inquired into 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 inquired about managing access to networks and network services, and we have inspected the solution. We have inspected a number of users, in order to establish that they only have access to approved networks and services, based on work-related requirements.	No deviations noted.

A.9.2 User access management

Control objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

No	Lessor Group's control	REVI-IT's test	Test results
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inquired into the procedure for creating and aborting users and we have inspected the procedures. We have inspected a sample of documentation for user creation and removal of users.	No deviations noted.

No	Lessor Group's control	REVI-IT's test	Test results
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services.	We have inquired that a procedure for user administration has been established. We have inspected that the procedure for user administration has been implemented.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have 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.	We have observed that staff with access to the test environment also have access to move program changes into production and therefore functional separation between test- and production environments is not supported by separation of logical access rights to the environments. No further deviations noted.
9.2.5	*Review of user access rights* 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	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inquired into procedures about discontinuation and adjustment of access rights. We have inspected a sample of 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's control	REVI-IT's test	Test results
9.3.1	*Use of secret authentication information* Users are required to follow the organizations' 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 unauthorized access to systems and applications.**			
No	Lessor Group's control	REVI-IT's test	Test results
9.4.1	*Information access restriction* Access to information and application system functions is restricted in accordance with the access control policy.	We have inquired about guidelines and procedures restricting access to applications.	No deviations noted.

No	Lessor Group's control	REVI-IT's test	Test results
9.4.2	*Secure log-on procedures* Access to systems and applications is controlled by procedure for secure logon.	We have inquired about the secure logon procedure and we have inspected the solution.	No deviations noted.
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inquired that policies and procedures requires quality passwords. We have inquired that systems for administration of access codes are configured in accordance with the requirements.	No deviations noted.
9.4.4	*Use of privileged utility programs* The use of utility programs that might be capable of overriding system and application controls have been restricted and tightly controlled.	We have inquired into procedures to protect against bypassing of system- and application controls by using privileged utility programs.	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's control	REVI-IT'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 inquired into the policy of using encryption, and we have on a sample basis inspected the use of cryptography.	No deviations noted.

A.11 Physical and environmental security

A.11.1 Secure areas

Control objective: To prevent unauthorized physical access, damage and interference to the organisation's information and information processing facilities.

No	Lessor Group's control	REVI-IT'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 inquired into the procedure for physical security of facilities and security perimeters. We have inquired into 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 inquired into the procedures for access control to secure areas.	No deviations noted.

No	Lessor Group's control	REVI-IT's test	Test results
11.1.3	*Securing offices, rooms, and facilities* Physical security for offices rooms and facilities has been designed and applied.	We have inspected that physical security has been applied to protect offices, rooms, and facilities.	No deviations noted.
11.1.4	*Protection against external and environmental threats.* Physical protection against natural disasters, malicious attack or accidents should be designed and applied.	We have inspected procedures for protection against external and environmental threats.	No deviations noted.

A.11.2 Equipment

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

No	Lessor Group's control	REVI-IT's test	Test results
11.2.1	*Equipment sitting and protection* 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.
11.2.2	*Supporting utilities* Equipment is protected from power failures and other disruptions caused by failures in supporting utilities.	We have inspected the policy for supporting utilities. We have inspected the procedure for handling supporting utilities. We have inspected service rapport for supporting utilities.	No deviations noted.

No	Lessor Group's control	REVI-IT's test	Test results
11.2.3	*Cabling security* Power telecommunications cabling carrying data or supporting information services are protected from interception, interference, or damage.	We have inspected the policy for cabling security to ensure that relevant cabling has been identified. We have inspected relevant power/telecommunications cabling, carrying data to ensure that it is secure.	No deviations noted.
11.2.4	*Equipment maintenance* Equipment is correctly maintained to ensure its continued availability and integrity.	We have inspected the procedure for maintenance of equipment and ensures that equipment continuously maintained.	No deviations noted.
11.2.7	*Secure disposal or re-use of equipment* All items of equipment containing storage media have been verified to ensure that any sensitive data and licensed software have been removed or securely overwritten prior to disposal or re-use.	We have inquired into the procedure for deletion of data and software on storage media, before disposing of same. We have inspected a selection of equipment, in order to establish whether data and software had been deleted before disposal.	No deviations noted.
11.2.8	*Unattended user equipment* Users are ensuring that unattended equipment has appropriate protection.	We have inquired into the procedure for protection of unattended equipment.	No deviations noted.
11.2.9	*Clear desk and clear screen policy* A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities is adopted.	We have inquired into the policy of tidy desk and clear screen.	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's control	REVI-IT's test	Test results
12.1.1	*Documented operating procedures* Operating procedures have been documented and made available to all users.	We have inquired about requirements for documentation and maintenance of operating procedures. We have inquired 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 inquired about the procedure regarding changes of information handling equipment and -systems. We have inquired whether a selection of changes, made on platforms, databases and network equipment have been approved, tested, documented and implemented in the production environment, according to the Change Management procedure. We have inspected servers, database systems and network components, in order to find examples of actual changes made, and locate documentation that Change Management procedure has been followed.	We have observed that staff with access to the test environment also have access to move program changes into production and therefore functional separation between test- and production environments is not supported by separation of logical access rights to the environments. No further deviations noted.
12.1.3	*Capacity management* The use of recourses is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inquired into the procedure for monitoring use of recourses 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.

No	Lessor Group's control	REVI-IT's test	Test results
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 inquired into securing the separation of development-, test- and operations facilities. We have on a sample basis inspected, that development, test, and production are either physically or logically separated.	We have observed that staff with access to the test environment also have access to move program changes into production and therefore functional separation between test- and production environments is not supported by separation of logical access rights to the environments. No further 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's control	REVI-IT'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 inquired into measures against malware. We have inquired about the use of antivirus software and we have inspected documentation for its use.	No deviations noted.

A.12.3 Backup

Control objective: To protect against loss of data.

No	Lessor Group's control	REVI-IT'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 inquired into configuration of backup and we have inspected samples of documentation for the setup according to requirements. We have inspected that backup is monitored. We have inquired about testing of backupfile recovery 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's control	REVI-IT's test	Test results
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events have been produced, kept, and regularly reviewed.	We have inquired into user activity logging. We have inspected samples of logging configurations.	No deviations noted.
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have 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.

No	Lessor Group's control	REVI-IT's test	Test results
12.4.3	*Administrator and operator logs* 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 inspected logon setups on chosen servers and database systems, in order to establish whether the actions of system administrators and operators are logged.	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 inquired into 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's control	REVI-IT's test	Test results
12.5.1	*Installation of software on operational systems* Procedures are implemented to control the installation of software on operational systems.	We have inquired about software installation guidelines on operating systems and we have 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's control	REVI-IT'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 inquired into 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 inquired into 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's control	REVI-IT's test	Test results
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	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. We have inspected documentation for network design and a range of security setups of network components, in order to establish whether the defined rules and regulations have been implemented.	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 observed that written requirements about security mechanisms, service levels and management requirements of all network services are present. We have inspected a range of network components in order to estimate whether the components have been set up according to requirements and contractor's re-commended baselines.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inquired into the guidelines for segregation of networks.	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's control	REVI-IT's test	Test results
13.2.1	*Information transfer policies and procedures* Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.	We have inquired about data transfer policies and procedures.	No deviations noted.
13.2.2	*Agreements on information transfer* Agreements address the secure transfer of business information between the organisation and external parties.	We have inquired about data transfer agreements. We have inquired into agreements with customers and other external parties, describing the requirements for safe exchange of data.	No deviations noted.
13.2.3	*Electronic messaging* Information involved in electronic messaging is being appropriately protected.	We have inquired about guidelines for sending confidential information.	No deviations noted.
13.2.4	*Confidentiality or non-disclosure-agreements* 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.	We have inquired about the procedure for establishing non-disclosure-agreements. We have inspected a standard non-disclosure-agreement to establish whether the procedure has been followed when hiring of new staff and closing of agreements with consultants.	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's control	REVI-IT'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 inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities. In addition, we have inspected the procedure for handling 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 inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines.	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 events during the period and we have inspected these.	No deviations noted.

No	Lessor Group's control	REVI-IT's test	Test results
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 inquired into the procedure for assessment, response and evaluation of information security breaches.	No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inquired about whether information security incidents have been responded to, in accordance with the documented procedures.	No deviations noted.
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have 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's control	REVI-IT's test	Test results
17.1.1	*Planning information security continuity* The organisation has determined its requirements for information security and the continuity of information security management in adverse situations e.g. during a crisis or disaster.	We have inquired about 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	*Implementing information security continuity* The organisation has established document implementation and maintenance of processes procedures and controls to ensure the required level of continuity for information security during an adverse situation.	We have inquired about 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.
17.1.3	*Verify review and evaluate information security continuity* The organisation is verifying the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	We have inquired about test of the contingency plan and we have inspected documentation for tests performed. We have also inquired into reassessment of the contingency plan, and we have inspected documentation for reassessment.	No deviations noted.

A.17.2 Redundancies

Control objective: To ensure availability of information processing facilities.

No	Lessor Group's control	REVI-IT's test	Test results
17.2.1	*Availability of information security processing facilities* Information processing facilities have been implemented with redundancy sufficient to meet availability requirements.	We have inquired about the availability of operating systems and we have inspected the established measures.	No deviations noted.

A.18 Compliance

A.18.2 Information security reviews

Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.

No	Lessor Group's control	REVI-IT'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.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have inquired for internal controls to ensure compliance with security policies and procedures, and we have inspected selected controls.	No deviations noted.