# Independent service auditor's assurance report on the description of controls, their design and operating effectiveness regarding the operation of hosted services for the period 01-04-2015 to 31-03-2016

ISAE 3402-II

## LESSOR Group

April 2016

This report was originally prepared in Danish. In case of discrepancies, the Danish report is applicable.

# Table of contents

## Section 1: 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 01-04-2015 to 31-03-2016. 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 01-04-2015 to 31-03-2016
- (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 01-04-2015 to 31-03-2016. 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 01-04-2015 to 31-03-2016.

Allerød, 26 April 2016

LESSOR Group

Henrik Fich
CEO

# Section 2: LESSOR Group's description of control and hosting environment

## Introduction

The LESSOR Group is composed of:

- LESSOR A/S
- LESSOR GmbH
- Danske Lønsystemer A/S
- ilohngehalt internetservices GmbH
- ISALAIRE EURL
- NORLØNN AS
- Łatwe Płace Sp. z o.o.
- quickpayroll Ltd.
- Swelön AB
- Pagaveloce
- Hispanomina

The object of this description is to provide information to the customers of the LESSOR Group 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.

The description includes control objectives and audits conducted by the 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.

## Organisation and responsibility

The company is characterized by a clear and transparent company structure.

LESSOR Group employs approximately 100 employees. The organizational structure of the LESSOR Group includes the departments Administration, Economic and Operating Support 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

### Policies for information security

*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.

*Review of the policies for information security*

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

### Information security roles and responsibilities

*Allocation of information security responsibilities*

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.

*Segregation of duties*

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 device policy*

We have made it possible for our employees to work from home via a VPN connection with two-way-authentication. No equipment (portable computers etc.) must be left unattended. Portable units are protected by HDD passwords, login 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.

*Teleworking*

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 established cooperation with an external partner to ensure that we employ the right candidate with regard to background and skills.

*Terms and 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 responsibilities*

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.

*Information security awareness, education and training*

Our assets are first of all our employees. We encourage our operating staff to maintain 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.

*Disciplinary process*

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

*Inventory 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 a number of 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*

The 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, 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.

### Media handling

*Management of removable media*

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 policy

*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

*User registration and de-registration*

The user profiles of our customers are created solely due to the wishes of our customers. In some 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.

*Assignment of rights*

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

*Management of privileged access rights*

Personal login information is known only by the employee and subject to a password policy to ensure the complexity.

*Review 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 secret authentication information*

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. that cannot be used for logging in and which are not changed for systemic reasons are stored in a separate system. Only four members of the LESSOR Group can access this system.

### System and application access control

*Information access restriction*

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.

*Password management system*

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 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 and environmental security

*Secure areas*

The physical access to the data centre of the LESSOR Group in Allerød is limited to four 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 maintenance*

**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 by Alive Services 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 by Alive Services 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.

*Secure disposal or re-use 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 are centrally managed. Screens are locked after 10 minutes inactivity. Thus, we minimize the risk of unauthorized access to confidential data.

## Operations 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

*Controls 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

*Information backup*

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 recreate 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

*Event 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 log 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.

*Clock 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 (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 on-going risk assessments.

## Communications security

*Network controls*

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.

*Security of 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.

*Segregation in networks*

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

*Information transfer policies and procedures*

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

The communication with users is carried out via emails, support forums or, only rarely, via fax.

*Agreements on information transfer*

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

## System acquisition, development and maintenance

### Security requirements of information systems

*Information security requirements analysis and specification*

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.

*System change control procedures*

All changes follow an implemented change management process.

Our test and production environments are logically and physically separated.

*Restrictions on changes to software packages*

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 to supplier services*

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

## Information security aspects of business continuity management

*Information security continuity*

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.

*Verify, review and evaluate information security continuity*

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.

*Redundancies*

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 review 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 control procedures

LESSOR Groups customers are, unless otherwise agreed, responsible for establishing connection to servers of LESSOR Group. 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.

## Changes implemented during the period

The following changes have been implemented during the period:

- Improvement of patch management policies and procedures
- Introduction of a new log policy and improvement of the procedure
- Purchase of a new log server
- Implementation of centralized logging
- Improvement of procedures for the installation of new servers
- Replacement of Zabbix monitoring by CheckMK
- Implementation of new strong firewalls
- Purchase of DDoS Shield.

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

To the management of LESSOR Group, their customers and their auditors.

### Scope

We have been engaged to report on LESSOR Group's description, presented in Section 2. The description, as confirmed by the management of LESSOR Group in section one, covers LESSOR Group's operating and hosting services throughout the period 01-04-2015 to 31-03-2016, as well as the design and operation of the controls related to the control objectives stated in the description.

### LESSOR Group's responsibility

LESSOR Group is responsible for preparing the description (section 2) and the related statement (section 1) 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.

The firm applies International Standard on Quality Control 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

Based on our procedures, our responsibility is to express an opinion on LESSOR Group's description (section 2) as well as on the design and functionality of the controls related to the controls objectives stated in this description. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by IAASB. 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 judgment, 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, described in section 2.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

## Limitations of controls at a service organisation

LESSOR Group's description in section 2 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. Also, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

## 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 in the period throughout 01-04-2015 to 31-03-2016, is fair in all material respects

(b) the controls related to the control objectives stated in the description were suitably designed in the entire period throughout 01-04-2015 to 31-03-2016 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 01-04-2015 to 31-03-2016.

## 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 statements.

Copenhagen, 26 April 2016

REVI-IT A/S
State authorised public accounting firm

| | |
|---|---|
| Henrik Paaske<br>State Authorised Public Accountant | Martin Brogaard Nielsen<br>IT Auditor, CISA, CRISC, CEO |

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

The following overview is provided to facilitate an understanding of the effectiveness of the controls implemented by LESSOR Group. Our testing of functionality comprised the controls that we considered necessary to provide reasonable assurance that the control objectives stated in the description were achieved during the period 01-04-2015 to 31-03-2016.

Thus, we have not necessarily tested all the controls mentioned by LESSOR Group in the description in Section 2.

Moreover, our statement does not apply to any controls performed at LESSOR Group's customers, as the customers' own auditors should perform this review and assessment.

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

| Method | General description |
|---|---|
| Enquiry | Interview, i.e. enquiry with selected personnel at the company regarding controls |
| Observation | Observing how controls are performed |
| Inspection | Review and evaluation of policies, procedures, and documentation concerning the performance of controls |
| Re-performing control procedures | We have re-performed – or have observed the re-performance of –controls in order to verify that the control is working as assumed |

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.

# Risk assessment and management

## Risk assessment

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 4.1 | To ensure that the company periodically performs an analysis and assessment of the IT risk profile. | We have enquired about the preparation of an IT risk analysis, and we have inspected the prepared IT risk analysis.<br>We have enquired about review of the IT risk analysis, and we have inspected documentation for review during the audit period. | No significant deviations noted. |

# Information security policies

## Management direction for information security

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 5.1 | To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations. | We have enquired about the preparation of an information security policy, and we have inspected the document.<br>We have enquired about review of the IT security policy, and we have inspected documentation for review during the audit period.<br>We have enquired about the management's approval of the information security policy, and we have inspected documentation for management approval. | No significant deviations noted. |

## Organisation of information security

### Internal organisation

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 6.1 | To establish a management framework to initiate and control the implementation and operation of information security within the organisation. | We have enquired about the allocation of responsibilities for information security, and we have inspected documentation for the allocation of responsibilities.<br>We have enquired about segregation of duties, and we have inspected documentation for segregation of duties.<br>We have enquired about guidelines for contact with authorities.<br>We have enquired about contact with interest groups, and we have inspected documentation for contact.<br>We have enquired about the decision on information security in connection with project management, and we have inspected the project model. | No significant deviations noted. |

### Mobile devices and teleworking

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 6.2 | To ensure the security of teleworking and use of mobile devices. | We have enquired about the management of mobile devices, and we have inspected the solution.<br>We have enquired about the security of teleworking, and we have inspected the solution. | No significant deviations noted. |

## Human resource security

### Prior to employment

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 7.1 | To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. | We have enquired about a procedure for screening new employees, and we have inspected the procedure.<br>We have in spot checks inspected documentation for the procedure being followed.<br>We have enquired about the formalisation of terms of employment, and we have in spot checks inspected documentation for the formalisation of terms of employment. | No significant deviations noted. |

### During employment

| | | | |
|---|---|---|---|
| 7.2 | To ensure that employees and contractors are aware of and fulfil their information security responsibilities. | We have enquired about the management's responsibility for disseminating information security criteria, and we have inspected the guidelines for dissemination.<br>We have enquired about further training of employees, and we have in spot checks inspected documentation for further training.<br>We have enquired about guidelines for disciplinary processes, and we have inspected the guidelines. | No significant deviations noted. |

### Termination and change of employment

| | | | |
|---|---|---|---|
| 7.3 | To protect the organisation's interests as part of the process of changing or terminating employment. | We have enquired about the formalisation of obligations applicable after the termination of employees.<br>We have in spot checks inspected documentation for the matter. | No significant deviations noted. |

## Asset management

### Responsibility for assets

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 8.1 | To identify organisational assets and define appropriate protection responsibilities. | We have enquired about inventories of assets, and we have in spot checks inspected inventories of assets.<br>We have enquired about ownership of assets, and we have inspected the allocation of ownership of assets.<br>We have enquired about guidelines for acceptable use of assets, and we have inspected these guidelines.<br>We have enquired about a procedure for securing the return of assets, and we have inspected the procedure.<br>We have in spot checks inspected documentation for the return of assets. | No significant deviations noted. |

### Information classification

| | | | |
|---|---|---|---|
| 8.2 | To ensure that the information receives an appropriate level of protection in accordance with its importance to the organisation. | We have enquired about guidelines for the classification and labelling of data, and we have inspected the guidelines.<br>We have enquired about guidelines for data management, and we have inspected the guidelines. | No significant deviations noted. |

### Media handling

| | | | |
|---|---|---|---|
| 8.3 | To prevent unauthorised disclosure, modification, removal or destruction of information stored on media. | We have enquired about guidelines for the use of removable media, and we have inspected the guidelines.<br>We have enquired about the disposal of media, and we have inspected documentation for secure disposal.<br>We have enquired about a procedure for protecting removable media during transport, and we have inspected the procedure. | No significant deviations noted. |

## Access control

### Business requirements of access control

| No. | Control objective | REVI-IT’s test | Test results |
|---|---|---|---|
| 9.1 | To limit access to information and information processing facilities. | We have enquired about policies for managing access to systems and premises, and we have inspected the policies.<br>We have enquired about procedures for managing access to network and network services, and we have inspected selected procedures. | No significant deviations noted. |

### User access management

| | | | |
|---|---|---|---|
| 9.2 | To ensure authorised user access and to prevent unauthorised access to systems and services. | We have enquired about a procedure for user management, and we have inspected the procedure.<br>We have enquired about a procedure for the allocation of rights, and we have inspected the procedure.<br>We have in spot checks inspected documentation for the creation of users and allocation of rights.<br>We have enquired about control with privileged rights, and we have inspected selected controls.<br>We have enquired about a process for the disclosure of logon information, and we have inspected the process.<br>We have enquired about periodic review of users, and we have inspected documentation for review during the audit period.<br>We have enquired abut a procedure for revoking access rights, and we have inspected the procedure.<br>We have in spot checks inspected documentation for timely revocation of access rights. | During some parts of the audit period there has not been a formal procedure for user creation.<br>The matter has been remedied in September 2015. |

### User responsibilities

| | | | |
|---|---|---|---|
| 9.3 | To make users accountable for safeguarding their authentication information. | We have enquired about guidelines for managing confidential passwords, and we have inspected the guidelines. | No significant deviations noted. |

### System and application access control

| | | | |
|---|---|---|---|
| 9.4 | To prevent unauthorised access to systems and applications. | We have enquired about restricted access to data, and we have inspected documentation for restriction.<br>We have enquired about a procedure for logon, and we have inspected the solution for adequate security.<br>We have enquired about a system for the administration of passwords, and we have in spot checks inspected requirements for password quality.<br>We have enquired about the use of privileged system tools.<br>We have enquired about the restriction of access to privileged system tools, and we have inspected documentation for restriction.<br>We have enquired about the management of access to source code, and we have inspected the solution. | No significant deviations noted. |

## Cryptography

### Cryptographic controls

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 10.1 | To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. | We have enquired about a policy for the use of cryptography, and we have inspected the policy.<br>We have enquired about a policy for the administration of encryption keys, and we have inspected the policy. | No significant deviations noted. |

# Physical and environmental security

## Secure areas

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 11.1 | To prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities. | We have enquired about a physical security perimeter at the company's premises, and we have inspected the solution in place.<br>We have enquired about access controls for securing offices, rooms and operations facilities, and we have inspected selected access controls.<br>Additionally, we have inspected the procedure for allocation of access to premises critical to operations.<br>We have inspected LESSOR Group's offices in order to check the physical security.<br>We have inspected security for mitigating external and environmental threats.<br>We have enquired about an area for the delivery of parcels and goods. | No significant deviations noted. |

## Equipment

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 11.2 | To prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations. | We have enquired about the placement of operations equipment, and we have inspected the physical circumstances for protecting operations equipment.<br>We have enquired about the use of supporting supplies, and we have inspected areas critical to operations and have verified the existence of supporting supplies.<br>We have enquired about the protection of cables in the data centre, and we have physically inspected the solution.<br>We have enquired about maintenance of equipment critical to operations, and we have inspected documentation for maintenance and test of equipment critical to operations during the period.<br>We have enquired about a policy for the disposal of media and equipment carrying data, and we have inspected the policy. Additionally, we have inspected documentation for secure disposal of media carrying data.<br>We have enquired about protecting unsupervised user equipment, and we have inspected documentation for the protection.<br>We have enquired about a policy for clean desk and screen, and we have inspected the policy. | No significant deviations noted. |

## Operations security

### Operational procedures and responsibilities

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 12.1 | To ensure correct and secure operation of information processing facilities. | We have enquired about documented operations procedures, and we have in spot checks inspected the procedures.<br>We have enquired about a procedure for change management, and we have inspected the procedure.<br>We have in spot checks inspected documentation for the procedure being followed.<br>We have enquired about capacity management and monitoring, and we have inspected documentation for management and monitoring.<br>We have enquired about segregation of development, test, and operations facilities, and we have inspected documentation for segregation. | No significant deviations noted. |

### Protection from malware

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 12.2 | To ensure that information and information processing facilities are protected against malware. | We have enquired about measures to protect against malware, and we have inspected the management.<br>We have enquired about the use of anti-virus on user equipment, and we have in spot checks inspected documentation for the use of anti-virus. | No significant deviations noted. |

### Backup

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 12.3 | To protect against loss of data. | We have enquired about a procedure for setup and execution of backup, and we have inspected the procedure.<br>We have enquired about documentation for the setup of backup, and we have inspected documentation for the setup.<br>We have enquired about backup retention, and we have inspected documentation for setup.<br>We have enquired about controls for the execution of backup, and we have inspected the control.<br>We have enquired about documentation for test of restore, and we have inspected documentation for test of restore. | No significant deviations noted. |

### Logging and monitoring

| | | | |
|---|---|---|---|
| 12.4 | To record events and generate evidence. | We have enquired about logging, and we have in spot checks inspected logging configuration.<br>We have enquired about the protection of log information throughout the period, and we have inspected the solution.<br>We have enquired about clock synchronisation on the network, and we have in spot checks inspected documentation for clock synchronisation. | System-related events are logged and followed up upon. However, a control has not been implemented for following up on user-related events.<br>We have observed that a new system has been implemented in Q1 2016 for logging and following up upon user-related and system-related events. |

### Control of operational software

| | | | |
|---|---|---|---|
| 12.5 | To ensure the integrity of operational systems. | We have enquired about the installation of programs and updates on operational systems, and we have inspected the procedure.<br>We have in spot checks inspected documentation for updates to operational systems. | No significant deviations noted. |

### Technical vulnerability management

| | | | |
|---|---|---|---|
| 12.6 | To prevent exploitation of technical vulnerabilities. | We have enquired about the management of technical vulnerabilities, and we have inspected the established precautions.<br>We have enquired about restrictions to installing programs, and we have inspected the established precautions. | No significant deviations noted. |

## Communications security

### Network security management

| No. | Control objective | REVI-IT’s test | Test results |
|---|---|---|---|
| 13.1 | To ensure the protection of information in networks and its supporting information processing facilities. | We have enquired about precautions for protecting the network and network services, and we have inspected the established precautions.<br>We have enquired about network segregation, and we have inspected documentation for the segregation. | No significant deviations noted. |

### Information transfer

| | | | |
|---|---|---|---|
| 13.2 | To maintain the security of information transferred within an organisation and with any external entity. | We have enquired about a policy for information transfers, and we have inspected the policy.<br>We have enquired about the use of secure connections when transferring information, and we have inspected documentation for the use of secure connections.<br>We have enquired about the establishment of confidentiality agreements, and we have in spot checks inspected documentation for the establishment. | No significant deviations noted. |

## Information security incident management

### Management of information security incidents and improvements

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 16.1 | To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. | We have enquired about a procedure for the management of information security incidents, and we have inspected the procedure.<br>We have enquired about allocation of responsibilities in connection with information security incidents, and we have inspected documentation for the allocation of responsibilities.<br>We have enquired about the reporting of information security incidents and weaknesses, and we have inspected the procedure for reporting.<br>We have enquired about assessment and management of information security incidents, and we have in spot checks inspected documentation for assessing and managing information security incidents.<br>We have enquired about learning from information security incidents, and we have in spot checks inspected the process.<br>We have enquired about the collection of evidence in connection with security breaches, and we have inspected the process for the collection of evidence. | No significant deviations noted. |

# Information security aspects of business continuity management

## Information security continuity

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 17.1 | Information security continuity should be embedded in the organisation's business continuity management systems. | We have enquired about the preparation of an information security continuity plan for ensuring the continuation of operations in connection with failures and similar, and we have inspected the continuity plan.<br>We have inspected documentation for test of the continuity plan during the period, and we have inspected documentation for the test. | No significant deviations noted. |

## Redundancies

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 17.2 | To ensure availability of information processing facilities. | We have enquired about adequate redundancies for maintaining accessibility to operational systems, and we have in spot checks inspected documentation for redundancies. | No significant deviations noted. |

# Compliance

## Information security reviews

| No. | Control objective | REVI-IT's test | Test results |
|---|---|---|---|
| 18.2 | To ensure that information security is implemented and operated in accordance with the organisational policies and procedures. | We have enquired about an independent review of the information security.<br>We have enquired about internal controls for ensuring compliance with policies and procedures, and we have in spot checks inspected documentation for internal controls.<br>We have enquired about periodic self-regulation of security configurations, and we have inspected documentation for the self-regulation. | No significant deviations noted. |