REVI-IT
IT-REVISION & RÅDGIVNING

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 1 April 2014 to 31 March 2015

ISAE 3402-II

LESSOR Group

REVI-IT A/S

Table of contents

Section 1: LESSOR Group's assertion

The accompanying 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 for customers throughout the period 1 April 2014 – 31 March 2015. The criteria used in this assertion were that the accompanying description:

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

- The types of services provided, when relevant
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for 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 (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions

(ii) Includes relevant details of changes to the service organisation's system throughout the period 1 April 2014 to 31 March 2015

(iii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 April 2014 to 31 March 2015. The criteria used in making this assertion were that:

(i) The risks that threated 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 individuals who have the appropriate competence and authority, throughout the period 1 April 2014 to 31 March 2015

We have improved our internal policies and processes during the audit period. However, not all conditions have been finally implemented, including documentation for access management for administrative, internal users, as well as implementation of a process for logging the before-mentioned user accesses. It is our plan to work on the mentioned conditions during Q3 2015.

Allerød, 8 May 2015

LESSOR Group

Henrik Fich
CEO

Section 2: LESSOR Group’s description of controls in connection with operation of their hosting services

Introduction – the LESSOR Group

The LESSOR Group consists 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 S.R.L.
- Hispanómina S.L.

The LESSOR Group has since 1972 supplied small, medium-sized and large companies with efficient and flexible IT solutions for PAYROLL, TIME & ATTENDANCE and HR. All solutions are developed to facilitate the everyday work of the customers. Today, more than 27,000 Danish and 1,500 international companies use one or more of the solutions of the LESSOR Group.

Description of the services included in this control description

LESSOR-5 (hosted solution), payroll system

LESSOR-Workforce, shift scheduling system (previously known as eGruppe)

Danløn, payroll system for smaller companies

The LESSOR-Portal, web based employee portal

European web payroll (ewp), payroll systems for smaller companies in Europe (pt. Sweden, Norway, Germany, France, Poland, Italy and Spain)

Control Environment

The LESSOR Group has established a control environment based on the ISAE 3402 report, which itself is based on the control frame of Annex a of ISO 27001, as well as on the management’s focus on best practices for day-to-day business functions. Below are listed the key elements constituting the control environment of the LESSOR Group:

- Risk assessment and management
- Security policy
- Organization of information security
- Security in relation to recruitment of new staff
- Asset management
- Access control
- Cryptography

- Physical and environmental security
- Operational safety
- Communication security
- Acquisition, development and maintenance
- Supplier relationships
- Security incident management
- Error correction procedure
- Reviews and audits

Risk Assessment and Management

The ISO team of the LESSOR Group has produced a risk analysis. On an annual basis or in case of significant changes, the team carries out a risk assessment of the assets of the LESSOR Group. Internal as well as external factors are being considered.

The risk analysis includes an assessment of all risk identified. The analysis will be updated on an annual basis or in case of significant changes.

Security Policy

The LESSOR Group has developed a security policy based on the risk analysis and approved by the CEO of the LESSOR Group. The policy is being reviewed at least once a year.

Organization of Information Security

The employees have the possibility of working from home via a VPN two-way authentication. The portable laptops handed out to the employees are all secured by a HDD password and hardware encrypted.

Security in Relation to Recruitment of New Staff

The LESSOR Group has prepared a procedure for the introduction of new staff which ensures that all employees are familiar with the security policy of the company as from the first day.

Asset Management

The complete infra-structure in the data center is documented and all equipment is described accurately. All documentation is being updated continuously.

Access Control

Administrative rights have been assigned to employees whose function requires access to the servers. On termination of employment, the user profiles and all rights connected to these profiles will be deleted.

Rules have been defined for password management, and all user profiles are continuously being reviewed.

Cryptography

The handing over of keys to the employees is documented in the HR system of the LESSOR Group.

Physical Security

All employees and cooperating partners dealing with the hosted services of the LESSOR Group must sign an undertaking of secrecy. The LESSOR Group has appointed an employee who is responsible for the complete management as regards IT security.

Access Control

Only four persons from the LESSOR Group are allowed physical access to LESSOR Group's data center in Allerød while a minimum number of employees are allowed remote access. External partners whose task is to service the equipment in the data center are always accompanied by an employee of the LESSOR Group.

Fire Safety

The LESSOR Group's data center is protected against fire by two INERGEN® systems – one in each server room. Regular reviews are carried out to ensure that all systems operate correctly. The LESSOR Group has made a service contract with the supplier including two annual servicing visits. In addition to that, all systems are continuously monitored by Alive Services for operational errors.

Data Center Cooling

In the LESSOR Group's data center, 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 systems operate correctly. The LESSOR Group has made a service contract with the supplier including four annual servicing visits. In addition to that, all systems are continuously monitored by Alive Services for operational errors.

Back-up Power (UPS units and generator)

In the LESSOR Group's data center, 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. The LESSOR Group has made a service contract with the respective suppliers including an annual inspection of both the UPS units and the standby system. In addition to that, both the UPS units and the standby generator are continuously monitored by Alive Services for operational errors.

Monitoring

The entrance to the data center is equipped with an alarm system and under video surveillance. All LESSOR Group hosting services including the infra-structure are monitored. The monitoring has been described and is being maintained continuously.

Operational Safety

The LESSOR Group has implemented processes monitoring all daily backups operations. Regular tests of restore procedures are being conducted.

Communication Security

The customers access the systems via public http/https.

Only approved network traffic (ingoing) will be allowed by the firewall. The complete firewall framework is regularly being reviewed by persons appointed by and employed in the LESSOR Group.

Acquisition, Development and Maintenance

Change management

All changes follow an implemented change management process.

Incident management

All incidents follow an implemented incident management process.

Event management

All events follow an implemented event management process.

Supplier Relationships

Formal agreements about the supply of internet connections and the inspection of all equipment in the data center have been entered with our cooperating partners.

Security Incident Management

The LESSOR Group monitors security incidents such as computer virus outbreaks as well as the best-known internet attacks. If a threat to the LESSOR Group is being identified, the threat will be subject to a thorough assessment. On this basis, it will be further evaluated what action to take.

Error Correction Procedure

The LESSOR Group has worked out a procedure for correction of errors on servers, in infra-structure etc. on different levels.

Reviews and Audits

We carry out an annual review of the information security.

We perform annual audits to ensure that internal policies and procedures are respected.

We are being evaluated by an external IT auditor in connection with the preparation of the annual ISAE 3402 statement.

Complementary controls

Unless otherwise agreed, LESSOR Group’s customers are responsible for establishing a connection to LESSOR Group’s servers. Furthermore, unless otherwise agreed, LESSOR Group’s customers are responsible for:

- Administration of their own users
- Their own internet connection
- Their own data in the system

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

It is our purpose to issue an assurance report on LESSOR Group's description, presented in section 2. The description, confirmed in section 1 by the management of LESSOR Group, encompasses the company's handling of customer transactions in relation to the company's hosting activities in the period 1 April 2014 to 31 March 2015, as well as the design and functionality of the controls related to the control objectives mentioned in the description.

This assurance report is prepared according to the inclusive method, and thus comprises the management's description of control objectives and related control activities with LESSOR Group for all areas of the general IT controls attributed to the delivered services.

LESSOR Group's responsibility

LESSOR Group is responsible for the preparation of the description (section 2) and associated assertion (section 1), including the completeness, accuracy and the way in which the description and assertion is presented. Additionally, LESSOR Group is responsible for delivering the services that the description covers; for stating the control objectives; and for the design, implementation and effectiveness of operating controls for obtaining the stated control objectives.

REVI-IT A/S' responsibility

On the basis of our actions, it is our responsibility to issue a conclusion regarding LESSOR Group's description (section 2) and regarding the design and functionality of the controls related to the control objectives stated in this description. We have performed our work in accordance with ISAE 3402, "Assurance reports on controls at a service organisation", issued by IAASB. This standard requires that we comply with ethical requirements and plan as well as perform our actions in order to ensure a high degree of certainty that the description in all material respects is accurate, and that the controls in all material respects are adequately designed and function effectively.

The task of issuing an assurance report with certainty for the description, design and functionality of controls with a service provider comprises performing a number of actions in order to achieve evidence for the information in the service provider's description of their system and for the design and functionality of the controls. The chosen actions depend on the auditor of the service provider's assessment, including the assessment of the risks that the description is not accurate, and that the controls are not adequately designed or do not function effectively. Our actions have included testing the functionality of those controls, which we consider necessary for ensuring a high degree of certainty that the control objectives mentioned in the description were achieved.

Furthermore, issuing an assessment with this degree of certainty requires an assessment of the complete presentation of the description, the appropriateness of the objectives stated herein as well as the appropriateness of the criteria, which the service provider has specified and described in section 2.

It is our opinion that the obtained evidence is sufficient and appropriate for forming the basis of our conclusion.

Limitations in controls at a service provider

LESSOR Group's description in section 2 is prepared in order to satisfy the usual requirements from a broad range of customers and their auditors, and thus do not necessarily include all aspects of the system that each customer could consider necessary for their specific situations. Furthermore, controls at a service provider may, due to their nature, not prevent or uncover all errors or omissions in the treatment or reporting of transactions. Additionally, the projection of any assessment of the functionality for future periods is subject to the risk that controls at a service provider can become inadequate or simply fail.

Conclusion

Our conclusion is formed on the basis of the circumstances accounted for in this assurance report. The criteria that we have used when forming our conclusion are the criteria described in LESSOR Group's description in section 2, and on the basis of this, it is our assessment that:

(a) the description of controls as they were designed and implemented in the entire period of 1 April 2014 to 31 March 2015, in all material respects are accurate
(b) the controls related to the control objectives mentioned in the description, in all material respects were adequately designed in the entire period of 1 April 2014 to 31 March 2015
(c) that the tested controls, which were the controls necessary to provide a high degree of certainty that the control objectives in the description were obtained in all material respects, have functioned effectively in the entire period of 1 April 2014 to 31 March 2015

Supplementary information

Without it effecting our conclusion, we are to draw attention to the management's assertion in section 1, where it is described that during the audit period there have been conditions that have not been finally implemented, including documentation for access management for internal, administrative users, as well as implementation of a process for logging for the aforementioned user accesses at LESSOR Group.

Description of test of controls

The specific controls that have been tested, as well as the type, the timing and results of these tests are provided in the subsequent main section (section 4).

Intended users and purpose

This assurance report is exclusively intended for customers that have used LESSOR Group's hosted services, and the auditors of these customers, who have the sufficient understanding to consider the description along with other information, including information of the customers' own controls. This information serves to obtain an understanding of the customers' information systems, which are relevant for the presentation of accounts.

Copenhagen, 8 May 2015

REVI-IT A/S
Statsautoriseret revisionsaktieselskab

Henrik Paaske
State Authorised Public Accountant

Martin Brogaard Nielsen
IT Auditor, CISA, CEO

Section 4: Control objectives, performed controls, tests and results thereof

The following overview is devised to create an understanding for the effectiveness of the controls that LESSOR Group has implemented. Our test of the functionality has comprised the controls that we have assessed to be necessary in order to obtain a high degree of certainty that the stated control objectives have been obtained in the period of 1 April 2014 to 31 March 2015.

Hence, we have not necessarily tested all the controls that LESSOR Group has mentioned in their description in section 2.

Additionally, controls performed at LESSOR Group's customers are not comprised by our assurance report, as the customers' own auditors should perform this review and assessment.

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

Method	Overall description
Enquiry	Interview, that is enquiring with selected personnel at the company regarding control
Observation	Observing how controls are performed
Inspection	Review of and evaluation of policies, procedures and documentation in relation to the performance of controls
Reperforming control procedures	We have performed – or observed – a reperformance of controls in order to verify that the control works as expected

The description and result of our tests in relation to the tested controls are evident in the following tables. To the extent that we have found material 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 result
4.1	The purpose is to ensure that the company periodically performs an analysis and assessment of the potential and relevant IT risks.	We have enquired about the preparation and maintenance of an IT risk analysis. We have inspected the risk analysis and control for periodic review.	We have not found any material deviations.

IT security management

IT security policy

No.	Control objective	REVI-IT's test	Test result
5.1	The purpose is to ensure that guidelines are issued in order to support the information security in accordance with business requirements and relevant laws and regulations.	We have enquired about the preparation of an IT security policy. We have inspected the policy and control for periodic review.	We have not found any material deviations.

Organisation of information security

Internal organisation

No.	Control objective	REVI-IT's test	Test result
6.1	The purpose is 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 IT security as well as about the documentation of segregation in the organisation. We have inspected the documentation for segregation of the organisation and areas of responsibility. We have enquired about the segregation of duties as well as inspected the guidelines for segregation of duties. We have enquired about contact with authorities and interest groups. We have inspected documentation for the contact with authorities and interest groups. We have enquired about the decisions regarding information security as a part of project management. We have inspected the procedure for change management.	We have not found any material deviations.
Mobile units and teleworking			
6.2	The purpose is to ensure the security of teleworking and use of mobile devices.	We have enquired about guidelines for the management of mobile devices and communication, and we have inspected the guidelines. We have enquired about the use of encryption in connection with external access to the systems, and we have observed the established solution.	We have not found any material deviations.

Human resource security

No.	Control objective	REVI-IT's test	Test result
Prior to employment			
7.1	The purpose is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.	We have enquired about the process and random sampling of documentation for the screening of employees prior to employment. We have enquired about the formalisation of the terms of employment and have by random sampling inspected the contents of employment contracts.	A comprehensive procedure for the process prior to employment has been formulated. However, there is no documentation for the screening of employees. The management has informed us that the matter will be remedied in Q2 2015.
During employment			
7.2	The purpose is to ensure that employees and contractors are aware of and fulfil their information security responsibilities.	We have enquired about a formal description of the management's responsibility and engagement in IT security matters. We have enquired about awareness and further training of the employees in information security and have inspected current guidelines.	We have not found any material deviations.
Termination and change of employment			
7.3	The purpose is to protect the organisation's interests as part of the process of changing or terminating employment.	We have enquired about the process in relation to the resignation/dismissal of employees, and we have inspected random samples of documentation in relation to this.	A comprehensive procedure for the process of resignation/dismissal of employees is in place. However, there is no documentation showing that this procedure is being followed. The management has informed us that the matter will be remedied in Q2 2015.

Asset management

Responsibility for assets			
No.	Control objective	REVI-IT's test	Test result
8.1	The purpose is to ensure identification of organisational assets and define appropriate protection responsibilities.	We have enquired about and have inspected an inventory of assets. We have enquired about guidelines for acceptable use of assets and have inspected current guidelines. We have enquired about a process for ensuring the return of previously issued assets at the termination of employment – and have by random sampling inspected the procedure for this.	There is a process in place for the return of assets at the termination of employment. However, this is not documented. The management has informed us that the matter will be remedied in Q2 2015.
Information classification			
8.2	The purpose is to ensure that information receives an appropriate level of protection in accordance with its importance to the organisation.	We have enquired about and have inspected guidelines for the classification of information. We have enquired about and have inspected guidelines for the management of assets.	We have not found any material deviations.
Media handling			
8.3	The purpose is to prevent unauthorised disclosure, modification, removal or destruction of information stored on media.	We have enquired about and have inspected the process for management of portable media. We have enquired about policies and have inspected guidelines for the disposal of media.	No media has been disposed of during the audit period. Therefore we cannot comment on the effectiveness of the control.

Access control

Business requirements of access control			
No.	Control objective	REVI-IT's test	Test result
9.1	The purpose is to limit access to information and information processing facilities.	We have enquired about and have inspected the policy for access control. We have enquired about and have inspected the management of access to networks and the configuration of network units.	We have not found any material deviations.

User access management			
9.2	The purpose is to ensure authorised user access and to prevent unauthorised access to systems and services.	We have enquired about and inspected procedures for providing and revoking access to systems. On the basis of the provided access lists we have selected random samples for the control of access provisioning and timely revocation of access. We have enquired about control with privileged access rights. We have enquired about and inspected guidelines for the management of confidential login information. We have enquired about the process for periodic review of users.	A comprehensive procedure for providing and revoking user access to systems is in place. However, there is no documentation that access provisioning and revocations have followed the established procedure. Additionally, there is no control for users with privileged access rights, and no control for periodic review of user rights. Moreover, we refer to the additional information in the service auditor's assessment regarding the management's assertion.
User responsibilities			
9.3	The purpose is to make users accountable for safeguarding their authentication information.	We have enquired about and have inspected guidelines for the use of confidential authentication information.	We have not found any material deviations.
System and application access control			
9.4	The purpose is to prevent unauthorised access to systems and applications.	We have enquired about the limitation of access to data and the procedure for secure login. We have observed the established procedure. We have enquired about and inspected the established system for managing passwords. We have enquired about the management of and access to source code.	We have not found any material deviations.

Cryptography

Policy on the use of cryptographic controls			
No.	Control objective	REVI-IT's test	Test result
10.1	The purpose is to ensure correct and effective use of cryptography in order to protect the confidentiality, authenticity and/or integrity of information.	We have enquired about and inspected the policy for use of cryptography and the administration of encryption keys. We have inspected the procedure and have observed the management of encryption keys.	We have not found any material deviations.

Physical and environmental controls

Secure areas			
No.	Control objective	REVI-IT's test	Test result
11.1	The purpose is to prevent unauthorised physical access, damage and interference to the organisation's information and information processing facilities.	We have enquired about and inspected the physical security perimeter. We have inspected the physical circumstances for protecting the access to operations facilities. We have enquired about and have inspected the protection of offices, premises and facilities. We have inspected the security measures established to mitigate external and environmental threats.	We have not found any material deviations.
Equipment			
11.2	The purpose is to prevent loss, damage, theft or compromise of assets and interruption to the organisation's operations.	We have enquired about and inspected the placement of the physical circumstances for adequate securing of the operational systems. We have enquired about supporting supplies and have inspected the solution for cases of power outages. We have enquired about and inspected the securing of cables in the data centre. We have enquired about and inspected documentation for maintenance of equipment in the data centre. We have enquired about the securing of equipment outside the company's premises. We have enquired about and inspected the policy for disposal of media and equipment containing data. We have enquired about the securing of user equipment without supervision and have inspected the established control. We have enquired about and inspected the policy for lock screens whenever the workstation is left unattended.	No media has been disposed of during the audit period. Therefore we cannot comment on the effectiveness of the control.

Operations security

Operational procedures and responsibilities			
No.	Control objective	REVI-IT's test	Test result
12.1	The purpose is to ensure correct and secure operations of information processing facilities.	We have enquired about documented operations procedures and have inspected controls for periodic review of these. We have enquired about change management and have by random sampling inspected documentation for changes in the audit period. We have enquired about and have observed the monitoring of capacity. Additionally, we have received documentation for monitoring. We have enquired about the segregation of development, testing, and operations facilities and have observed the segregation of these facilities.	We have not found any material deviations.
Protection against malware			
12.2	The purpose is to ensure that information and information processing facilities are protected against malware.	We have enquired about and have inspected measures against malware.	We have not found any material deviations.
Backup			
12.3	The purpose is to protect against loss of data.	We have enquired about setup, execution and archiving of backup. We have inspected the documentation for configuration and periodic restore of backup.	We have not found any material deviations.
Logging and monitoring			
12.4	The purpose is to record events and generate evidence.	We have enquired about logging of system and user activities. We have by random sampling inspected the logging configurations and have by random sampling inspected actions on system activities. We have enquired about the securing of log information in the audit period. We have enquired about clock synchronisation on the network and have inspected the documentation for synchronisation to an adequate clock server.	System activities are being logged and followed up. However, logging of user activities has not been implemented for internal, administrative users. Moreover, we refer to the additional information in the service auditor's assessment regarding the management's assertion.
Control of operational software			
12.5	The purpose is to ensure the integrity of operational systems.	We have enquired about and have inspected the procedure for installing applications on operational systems. We have by random sampling inspected the updating of servers.	Formal procedures for patching of servers exist. However, the procedure and control has only been effective since February 2015.

Technical vulnerability management			
12.6	The purpose is to prevent exploitation of technical vulnerabilities.	We have enquired about and have inspected the control in relation to timely update of the operational systems. We have by random samples inspected the documentation for monitoring and updates. We have enquired about limitations to installing applications and have inspected the measures in place.	Formal procedures for patching of servers exist. However, the procedure and control has only been effective since February 2015.

Communications security

Network security management			
NO.	Control objective	REVI-IT's test	Test result
13.1	The purpose is to ensure protection of information in networks and its supporting information processing facilities.	We have enquired about the securing of the network and have inspected the measures in place. We have enquired about and have inspected the securing of network services. We have enquired about and have inspected the network segregation.	We have not found any material deviations.
Information transfer			
13.2	The purpose is to maintain the security of information transferred within an organisation and with any external entity.	We have enquired about and have inspected policies for information transfer. We have enquired about the entering of agreements of confidentiality agreements and have by random samples inspected documentation for this.	We have not found any material deviations.

Information security incident management

Management of information security incidents and improvements

NO.	Control objective	REVI-IT's test	Test result
16.1	The purpose is 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 and have inspected the procedure for incident management and have observed that responsibilities are addressed in the procedure. We have enquired about the reporting of information security incidents and have by random sampling inspected documentation for adequate reporting and management of incidents. We have enquired about information security incidents in the audit period and have by random sampling inspected documentation for assessment, reaction, and reporting of information security incidents. We have enquired about and have inspected the process for learning from information security incidents. We have enquired about and have inspected the process for collecting evidence.	We have not found any material deviations.

Information security aspects of business continuity management

Information security continuity

NO.	Control objective	REVI-IT's test	Test result
17.1	The purpose is to ensure that information security continuity is embedded in the organisation's business continuity management systems.	We have enquired about the establishment of a contingency plan for securing business continuity in connection with failures and similar. We have inspected the plan and have, i.a., verified that has been updated in the audit period. We have enquired about documentation for test of the contingency plan in the audit period and have inspected the control for contingency testing.	We have not found any material deviations.
Redundancy			
17.2	The purpose is to ensure availability of information processing facilities.	We have enquired about the securing of the availability of operational systems. We have inspected the established redundancy precautions.	We have not found any material deviations.

Compliance

Information security reviews

N0.	Control objective	REVI-IT's test	Test result
18.2	The purpose is to ensure that information security is implemented and operated in accordance with the organisational policies and procedures.	We have enquired about independent review of the information security policy and have inspected the performed reviews. We have enquired about internal controls for ensuring compliance with security policy and procedures. We have inspected the internal audit of the organisation. We have enquired about periodic control of the security configurations and have inspected the documentation for performance of the control.	We have not found any material deviations.