Deloitte
Statsautoriseret Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
P.O. Box 1600
0900 Copenhagen C
Denmark

Phone +45 36 10 20 30
Fax +45 36 10 20 40
www.deloitte.dk

IT Relation A/S

ISAE 3402 Type 2

Independent auditor's report on general IT controls regarding operating and hosting services for 01.10.2014 to 30.09.2015

Contents

1. Independent auditor's report

To the management of IT Relation A/S, IT Relation A/S' customers and their auditors

Scope

We have been engaged to report on IT Relation A/S' assertions in section 2 and the related description of the system and control environment in section 3 with respect to IT Relation A/S' operating and hosting services, comprising design, implementation and effectiveness of controls as stated in the description. IT Relation A/S' description refers to the controls established to ensure the system security, data protection and operating efficiency of applications and the underlying infrastructure of the services, which IT Relation A/S offers operating and hosting customers (general IT controls).

This report is submitted using the partial method and does not cover controls that are carried out by IT Relation A/S' sub-service organization EnergiMidt. Controls performed by EnergiMidt include physical security and environmental mechanisms for securing the hardware.

IT Relation A/S' responsibilities

IT Relation A/S is responsible for preparing the accompanying assertion and the description of the system and control environment in section 3. IT Relation A/S is also responsible for ensuring the completeness and accuracy of the description, including a correct representation and presentation of such assertion and description in this report. IT Relation A/S is also responsible for providing the services covered by the description and for designing and implementing effective controls to achieve the identified control objectives.

Auditor's responsibilities

Based on our procedures, our responsibility is to express an opinion on IT Relation A/S' description as well as on the design, implementation and effectiveness of controls related to the control objectives stated in this description. We conducted our engagement in accordance with the International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board. This standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance that the description gives a fair presentation in all material aspects and that the controls have been appropriately designed and are operating effectively.

An assurance engagement relating to the description, design and effectiveness of controls at IT Relation A/S includes performing procedures to obtain evidence about IT Relation A/S' description of their system and about the design and effectiveness of the controls. The procedures selected depend on the auditor's judgment, including judgment of the risk that the description is not presented fairly

and that controls have not been suitably designed or do not function effectively. Our procedures include testing of the effectiveness of controls we consider necessary to provide reasonable assurance that the control objectives stated in the description will be achieved. Our procedures also include evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service provider and described in section 2.

We believe that the evidence obtained provides a sufficient basis for our opinion.

Limitations of controls at a service organization

IT Relation A/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 control of a system that each individual customer may consider important in their own particular control environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Moreover, the change in the assessment of effectiveness is subject to the risk that controls in a service organization may become insufficient or fail.

Furthermore, our opinion on subsequent periods' transactions will be subject to the risk that changes may have occurred in systems or controls or in the service organization's compliance with the policies and procedures described, which may cause our opinion to no longer be applicable.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 4.

Based on the audit performed, in our opinion, in all material respects:

a) The description of the general IT controls fairly presents IT Relation A/S' services of relevance to the system security, data protection and operating effectiveness for IT Relation A/S' customers such as designed and implemented in the period 01.10.2014 - 30.09.2015.
b) The controls related to the control objectives stated in the description were suitably designed in the entire period from 01.10.2014 - 30.09.2015.
c) The tested controls, which were the controls necessary to provide reasonable assurance that the control objectives in the description were achieved, have functioned effectively in the entire period from 01.10.2014 to 30.09.2015.

Description of tested controls

The specific controls tested and the nature, timing and results of those tests are evident from section 4.

Intended users and purpose

This report, the description of the system and control environment in section 3 and our tests of controls in section 4 are intended only for customers who have used IT Relation A/S' services and their auditors, who have a sufficient understanding to consider it along with other information, including information about the customers' own controls when identifying the risk of material misstatement of their financial statements.

Copenhagen, November 12, 2015

Deloitte

Statsautoriseret Revisionspartnerselskab

Steen Gellert-Kristensen
State Authorized Public Accountant

Michael Bagger
Manager, CISA

2. Assertions by IT Relation A/S

This report contains a description of the system and control environment, including the controls performed by IT Relation A/S for our customers under the contracts signed. Section 3 – IT Relation A/S' system description – describes the work processes established and the controls performed. The purpose of this report is to describe the processes and controls performed, which IT Relation A/S handles for our customers.

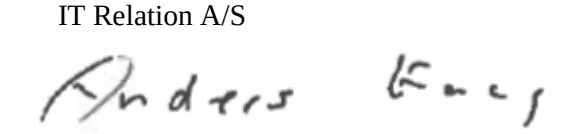
The description covers the period from 01.10.2014 to 30.09.2015 and is exclusively intended for IT Relation A/S' customers and their auditors.

IT Relation A/S confirms that:

- The descriptions adequately outline our work processes and controls performed to ensure satisfactory protective measures in respect to the operating and hosting services, including:
  - that a risk assessment procedure for identifying risks in hosting services has been defined
  - that based on risks control objectives have been defined and controls have been laid down to mitigate the risks identified
  - that the work processes and controls described have been implemented
  - that management monitored controls are in place to ensure effective implementation of the controls.
- The descriptions include relevant information about material changes in the services outsourced in the period from 01.10.2014 to 30.09.2015
- The descriptions have been prepared, taking into consideration that they must meet the common needs for information to be used in identifying risks in the financial statements of IT Relation A/S' customers

- The description of the controls performed has been appropriately designed, has been implemented at IT Relation A/S, and has functioned effectively in the entire period from 01.10.2014 to 30.09.2015, including:
    - that the controls established have been designed to mitigate the risks identified
    - that the controls established – if performed as described – will provide reasonable assurance that the risks identified are prevented or reduced to an acceptable level
    - that manual controls are performed by personnel with adequate skills and powers to do so.

Herning, November 12, 2015
IT Relation A/S



Anders Kaag
Consultant and Operations Manager

3. IT Relation A/S' system description

3.1 Introduction

This description has been prepared for the purpose of providing information to be used by IT Relation A/S' customers and their auditors in accordance with the requirements of the Danish Standard on Assurance Engagements regarding controls at a service organization, ISAE 3402. The description contains information about the system and control environment that has been established in connection with IT Relation A/S' operating and hosting services rendered to their customers.

The description comprises descriptions of the procedures used to safeguard satisfactory operation of systems. The purpose is to provide sufficient information for the hosting customers' auditors to independently assess the identification of risks of control weaknesses in the control environment so far as this may involve a risk of material misstatement in hosting customers' IT operations for the period from 01.10.2014 to 30.09.2015.

3.2 Description of IT Relation A/S' services

Since the establishment in 2003, IT Relation A/S has been part of the hosting business and has provided generations of IT solutions to many different industries in the market. In addition to hosting, IT Relation A/S also provides a wide range of other IT-related services.

IT Relation A/S offers the following services to the hosting market:

- Hosting and Housing
- Remote backup
- ServiceDesk

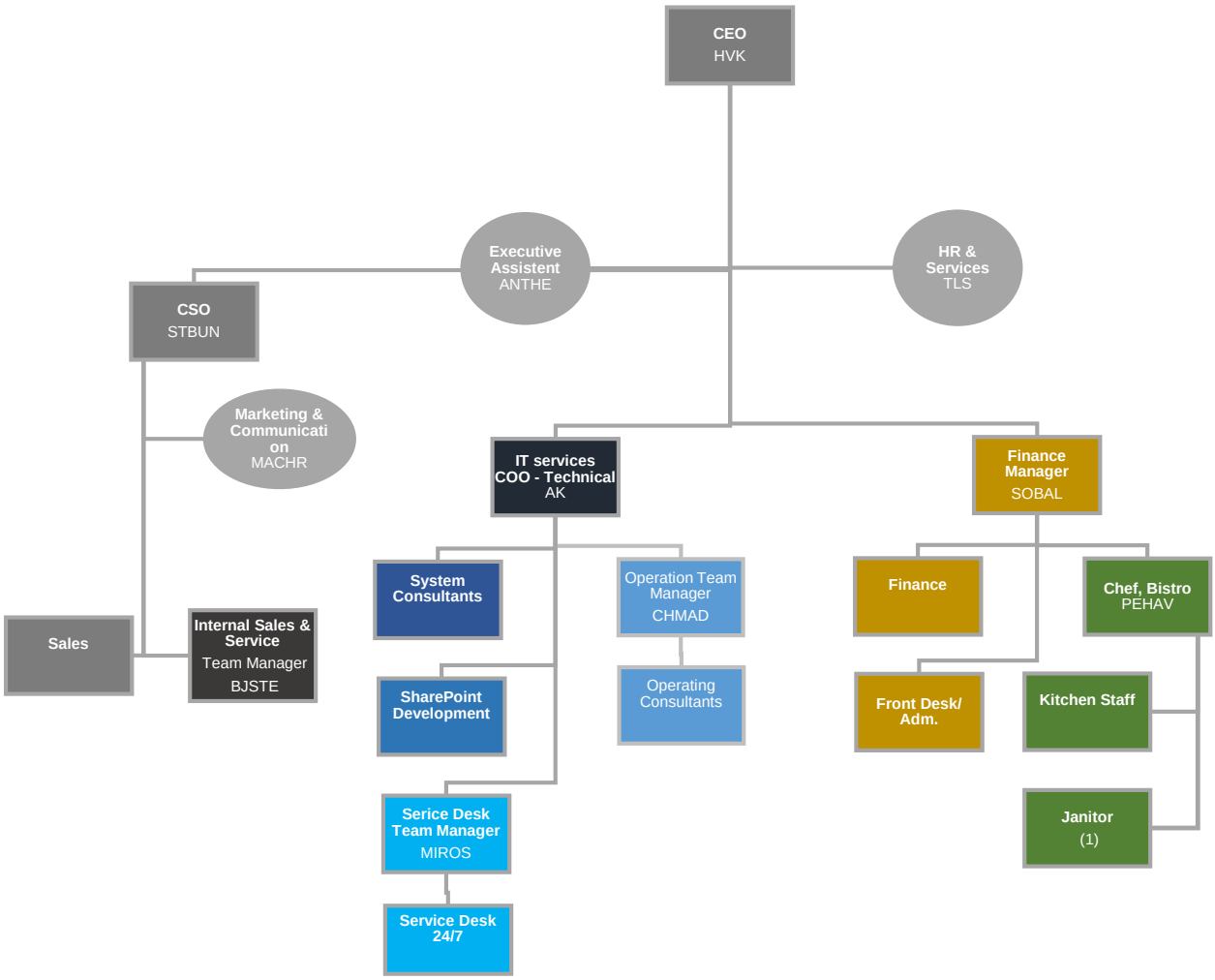
This system description includes a description of the work processes used and controls performed on the above services.

In addition to the above, IT Relation A/S also offers assistance in the following areas:

- Advisory services at CIO level
- Project management

3.3 IT Relation A/S' organization and security

The below organizational chart shows the responsibilities and organization of IT Relation A/S:



3.4 Risk management of IT Relation A/S

IT Relation A/S' risk management is performed in several areas and on several levels. Once a year, risk and threat assessment is carried out, which aims at internal systems in general. Input to this assessment is collected from the whole organization. The process is facilitated by the consultant and operations manager, who prepares drafts for IT Relation A/S' management. After the internal processing, the assessment is approved by IT Relation A/S' management.

In the project recommendation phase, a security assessment and an assessment of particular risks and uncertainties are prepared, depending on the nature of the project. This is made according to a predefined process.

At operational project level, a current risk management is performed. The risk management is performed according to an established project management model in which the responsibility for the project-related risk management is held by the project manager, who often chooses to include project participants, external partners and steering group members, if any, in the process.

3.5 Control framework, control structure and criteria for control implementation

IT Relation A/S' IT security policy, established processes and controls comprise all systems and services provided to customers. The continued work with adjusting and improving IT Relation A/S' security measures is performed currently in cooperation with highly qualified specialists.

As a member of BFIH, IT Relation A/S is also subject to an annual system/IT audit, which results in an annual auditor's report prepared in compliance with the ISAE3402 standard.

The determination of criteria for control implementation at IT Relation A/S is based on ISO27001/27002:2008. Based on this control framework, control areas and control activities have been implemented based on best practice to minimize the risk of services provided by IT Relation A/S. Based on the control model chosen, the following control areas are included in the overall control environment:

- Information security
- Internal organization of IT security
- Physical security
- Management of communication with customers
- Backup
- Operation and monitoring
- Access control
- Acquisition and maintenance of infrastructure
- Business Continuity Management

3.6 Established control environment

Each area has been described in detail in the following sections.

3.6.1 Information security

Objective

A management approved IT security policy has been prepared on the basis of an IT risk analysis and communicated to relevant employees in the enterprise.

Procedures and controls

IT Relation A/S identifies relevant IT risks to which the services established are subject. This is handled through a current threat and risk assessment at IT Relation A/S, partly in connection with all development projects and changes in system environments, and partly at an annual re-assessment of the risk analysis. The result of the annual review is presented to management.

IT Relation A/S also provides the hosting customers' auditors with a lot of information for their assessment of IT Relation A/S as a service organization. In addition to matters relating to operations, IT Relation A/S is also able to inform about security matters if required by the customers.

Time of performing the control

The IT security policy is reassessed at least once a year before performing IT audit and issuing a statement.

Who performs the control?

The annual review is performed by the security group.

Control documentation

The IT security policy is subject to version management.

3.6.2 Internal organization of IT security

Objective

To manage information security within the organization.

Procedures and controls

The Executive Board of IT Relation A/S, who is mainly responsible for the IT security, ensures that there are always procedures and systems supporting the compliance with the current IT security policy. The IT security group describes the overall objectives, and the operations manager is responsible for the preparation and implementation of relevant controls to observe the IT security policy. The security level must be measurable and controllable, where possible, and reflect best practice within the individual control activities in the service areas offered to the customers. At present, the IT security group consists of the following members:

- Consultant and Operations Manager Anders Kaag
- Team Manager of Operations Christian Bæk-Madsen

Time of performing the control

The group meets once a year to determine and follow up on objectives in relation to the IT security.

Who performs the control?

The annual review is performed by the security group.

Control documentation

The group documents their decisions when needed.

3.6.3 Physical security

IT Relation A/S has made an agreement with an external housing partner regarding the physical security of the company's IT environments. The agreement is made with EnergiMidt A/S. IT Relation A/S has full access to their customers' equipment placed at the housing partner. Controls performed by the external housing partner related to physical security are not included in the testing performed by Deloitte and is not part of this report.

Physical access control and security

Objective

The physical access to systems, data and other IT resources is limited to and planned with the hosting provider.

Procedures and controls

Access to the building is controlled through keys or electronic lock devices, which have been handed over to IT Relation A/S. Only persons who need to have access to the server room in the housing center have access to these keys. Finally, a key is required to get access to the rack cabinets used by IT Relation A/S. The list of the keys handed out is kept and updated by the hosting provider.

Time of performing the control

Key logs at IT Relation A/S are examined every week.

Who performs the control?

The operating department and the housing provider perform the control. Controls of handing out keys in general to the data center are not part of this report, and Deloitte has not performed any tests on these controls.

Control documentation

The individual user of the key from IT Relation A/S to the housing center records in the log when collecting and returning the keys.

Protection against environmental incidents

Objective

IT equipment is protected against environmental incidents such as power failure and fire.

Procedures and controls

The server room in the data center is protected against the following environmental incidents:

- Power failure
- Fire
- Climate

In all vital IT equipment, a stable current is ensured by an UPS installation, which is able to provide the systems with electricity until the generator has automatically started and is ready. The technical room and the server room are provided with smoke and temperature sensors, which are connected to the central fire surveillance system. The server room is also provided with automatic fire-fighting equipment (which is activated in case of too high values of either smoke or heat). These plants are subject to continuous maintenance.

The heat development in the server room is adjusted by the full-automatic cooling system, which ensures the correct temperature for stable operations and long durability of the IT equipment used. The plant is subject to continuous maintenance.

Time of performing the control

A daily visual control of the systems in housing is made by the providers.
The alarm system, ABA and UPS are inspected by our housing providers according to their 4400 statement.

Who performs the control?

The control is performed by the housing providers and providers of the other systems.

Control documentation

All control forms are located at the housing providers.

3.6.4 Management of communication with customers

ServiceDesk and customer support

Objective

There is adequate user support for users who contact the ServiceDesk, and the support agreed upon is provided within the area and time agreed upon.

Procedures and controls

IT Relation A/S has established a set of written ServiceDesk procedures in the areas agreed upon with the customer. The ServiceDesk procedures are prepared by ServiceDesk in close cooperation with the customer as well as third-party suppliers. Support to users is provided through the remote access software TeamViewer and through the platform tools of the terminal server.

Response time is agreed upon in the customer's SLA, and prioritizations are made in the case report system "Efecte".

Time of performing the control

On a daily basis, the ServiceDesk examines cases, which are waiting to be solved.

Who performs the control?

Controls are performed by ServiceDesk, and outside normal working hours they are performed by the ServiceDesk back office.

Control documentation

All incidents are logged in Efecte or ITR-TID.

Incident handling

Objective

Incident handling is performed satisfactorily based on the agreements made with customers, and IT Relation A/S checks that this is made in full compliance with the agreement and with the expected result.

Procedures and controls

IT Relation A/S uses ITR-TID to record and handle incidents, and the following is recorded:

- Errors (from email – "Efecte" (ServiceDesk) or from manual set-up)
- What has been done to mitigate errors
- Who has performed the assignment

- Time of incident registration
- Registration of time spent on the case (included in the operating agreement or to be invoiced).

The management of the operating department is responsible for monitoring that inquiries to ServiceDesk are prioritized and allocated resources and that incident handling is performed in accordance with customer agreements.

Time of performing the control

Incident handling is performed continuously throughout the day.

Who performs the control?

The incidents are handled by IT Relation A/S' operating department, and outside normal working hours, the incidents are handled by a consultant (back office).

Control documentation

All incidents are logged in ITR-TID. There is no automatic escalation etc. in ITR-TID to check the compliance with SLA agreements. The customers themselves have access to follow cases in the "SelfServiceportal".

3.6.5 Backup

Objective

A security copy of data is made and stored so the data can be restored if lost. IT Relation A/S checks whether the backup is performed without any errors, and in case of errors in the backup that an assessment of errors and a follow up of any errors are made.

Procedures and controls

A detailed description of the backup procedure has been prepared. The backup procedure is part of the daily operation and is thus automated in the system. Manual backup routines have been described in the operating procedures. The backup medium is changed by the operating department. The media are marked with a unique figure/bar code. The backup media are stored internally in the data fire safe.
The backup system is physically placed in another location than the hosting center (a distance of 20 km).

Backups are tested continuously, as backups are used to restore customer data. At the annual testing of the recovery procedures, the restore, in connection with a full restore of one single customer's environment, i.e. both system setup and user data, is verified.

Time of performing the control
Backup logs are checked during normal working hours.

Who performs the control?
The operating department handles the daily control of backup logs.

Control documentation
Daily operating check of the form and of the annual check form.
There is a log of which media is taken in and out of the data fire safe.

3.6.6 Operations and monitoring

Objective
It is monitored proactively that agreed-upon services are available, that available resources are in accordance with the agreed-upon standards/threshold values and that necessary jobs and runs, online as well as batches, are performed correctly and in due time. IT Relation A/S checks that this is fully made and with the expected result.

Procedures and controls
IT Relation A/S has established a set of written operating procedures for all material operating activities supporting the general expectations for a satisfactory operation as stated in IT Relation A/S' IT security policy. The operating procedures are prepared by the operating department in close cooperation with the customer, third-party providers and the operating department.

Operations are handled through the platform tools of the terminal server. There are a number of job descriptions for the operating department that lay down which surveillance and checks are performed daily, weekly and annually. Errors found in the controls performed and any errors from the systematic surveillance systems are corrected as soon as possible by means of procedures or best practice. The customer is currently informed about the extent and the implications of the errors observed.

The following functional areas have access to the customers' IT systems: ServiceDesk employees, operating employees and consultants.

Time of performing the control
The control is performed 24/7 or in the primary operating time according to the SLA agreement with the individual customer.

Who performs the control?
Controls are performed by IT Relation A/S' operating department, and outside normal working hours, the controls are performed by a consultant (back office).

Control documentation
All incidents are logged in ITR-TID or "Efecte".

3.6.7 Access control

Objective
Access to systems, data and other IT resources is managed, maintained and monitored consistently with the customers' requirements.
The access is divided into three areas:

- The customer's employee
- IT Relation A/S' employee
- Third-party consultants.

Procedures and controls
As a standard, a common system access is used for IT Relation A/S and the customer's internal IT employees (common administrator password). Third-party consultants are created as local administrators of the systems, which meet the customer's needs/requirements. Third-party consultants' accesses and rights to customer systems are only granted after a formal approval by the customer.

Generally, users are created on the basis of written inquires/emails to IT Relation A/S' operating department. It is IT Relation A/S who determines which of the pre-defined roles the users are to be assigned based on the customer's approval.

Rights to internal users at IT Relation A/S are created according to the same principles and approved by the consultant and operations manager. For internal employees, formal guidelines have been prepared relating to cancellation of users. These guidelines ensure, among other things, that a retired employee, when terminating his/her work at IT Relation A/S, returns keys and access cards, so that no physical access to the building can be obtained and the user ID cannot be used for log-in.

Time of performing the control
For customers, the control is performed when requested by the customer and when a third-party accedes to the customer's system.
Internally, control is made in connection with changes in staff.

Who performs the control?

For customers, it is the operating department of IT Relation A/S who is responsible for ensuring that the procedure for third-party access to the customer's environment is observed as agreed upon with the customer. For employees of IT Relation A/S, it is the consultant and operations manager who is responsible for who has access to what (customer environment – internal systems).

Control documentation

If a third party needs access to the customer's IT environment, it is the customer's IT manager who sends an authorization email to the operating department. This is then filed on the customer drive in the customer's operating file.

For IT Relation A/S' employees, the user forms are saved in the individual employee's staff file on the Executive Board drive.

3.6.8 Acquisition and maintenance of infrastructure

Network and communication software

Objective

Network and communication software is maintained and supported, and management ensures that changes or new acquisitions are made as required and that changes are tested and documented satisfactorily.

Procedures and controls

IT Relation A/S has full documentation for network and communication lines to the connected customers with whom there is an agreement on operations of the customer's network equipment.

IT Relation A/S currently assesses the need for upgrading firmware on network and communication software. To ensure stable operations, upgrades will only be made if necessary to ensure communication. Before changes are made, a backup copy is made of the configuration files for network components, and replaced equipment is kept for a certain period in case the new equipment does not function correctly or optimally. Significant changes in network configurations are made within the service windows agreed upon with the customers.

Time of performing the control

The control is performed in connection with upgrades and changes.

Who performs the control?

The network department is responsible for making upgrades and control of functionality.

Control documentation
Documentation is made in ITR-TID of tasks performed in the customer's system.

System software

Objective
System software is maintained and supported, and management ensures that changes or new acquisitions are made in accordance with the enterprise's needs and that changes are tested and documented satisfactorily.

Procedures and controls
For Windows servers, sufficient system documentation is obtained as required. IT Relation A/S has established procedures for the acquisition and updating of the system software on the Windows platforms. On the Windows platform, upgrades are provided by Microsoft and rolled out automatically on the servers through the Lumension patch management system. Thus, there is no manual assessment of these upgrades as the provider (Lumension) has tested and assessed the individual upgrades.

Time of performing the control
The control of upgrades is made through the Lumension patch management system, which contains logs for upgrades.

Who performs the control?
The operating department is responsible for making upgrades and control thereof.

Control documentation
Apart from the documentation in Lumension, logs are not made.

3.6.9 Business Continuity Management

Objective
To secure business activities and to protect critical business processes from the effects of major failures or disasters.

Procedures and controls
IT Relation A/S has defined an emergency plan so that the company's internal IT applications can continue in case of an emergency. The plan is reviewed on a regular basis.

Time of performing the control
The control of upgrades and test of emergency plan is performed annually.

Who performs the control?

The operating department is responsible for making upgrades and control thereof.

Control documentation

Review of emergency plans and test of procedures is documented when needed.

3.7 Additional information on the control environment

3.7.1 Matters to be considered by the customers' auditors

Services provided

The above system description of controls is based on IT Relation A/S' standard terms. Consequently, the customers' deviations from IT Relation A/S' standard terms are not comprised by this report. The customers' own auditors should therefore assess whether this report can be extended to the specific customer and identify any other risks, which are found material for the presentation of the customers' financial statements.

User administration

IT Relation A/S grants access and rights in accordance with customer instructions when these are reported to the ServiceDesk. IT Relation A/S is not responsible for this information being correct, and it is thus the customers' responsibility to ensure that the access and rights to the systems and applications are provided adequately and in compliance with best practice relating to segregation of duties.

IT Relation A/S also provides access to third-party consultants, primarily developers who are to maintain applications that are part of the hosting agreement. This is made according to instructions from IT Relation A/S' customers.

The customers' own auditors should therefore independently assess whether access and rights granted to applications, servers and databases to the customer's own employees as well as to third-party consultants are adequate based on an assessment of risks of misstatements in the financial reporting.

Emergency planning

The general conditions for hosting at IT Relation A/S do not define any requirements of emergency planning and restoring of the customers' system environment in case of an emergency. IT Relation A/S ensures general backup of customer environments, but a guarantee for a full restore of customers' system environment after an emergency is not comprised by the hosing agreements. The customers' own auditors should therefore independently assess the risks of lack of emergency planning and regular test thereof in relation to a risk of misstatement in the financial reporting.

Compliance with relevant legislation

IT Relation A/S has planned procedures and controls so that legislation in the areas for which IT Relation A/S is responsible is adequately observed. IT Relation A/S is not responsible for applications run on the hosted equipment, and consequently this report does not extend to assurance that adequate controls have been established in the user applications and that the applications observe the Danish Bookkeeping Act, the Danish Act on Processing of Personal Data or other relevant legislation.

External service provider

For control areas where the external housing partner EnergiMidt is responsible for performing the controls, the customers' own auditors should independently assess whether access to - and environmental protection of - the physical hardware has been appropriately implemented and maintained during the audit period.

4. Information provided by Deloitte

4.1 Introduction

This outline has been prepared in order to inform customers of controls performed by IT Relation A/S that may affect the treatment of accounting transactions and to state the effectiveness of the controls checked by us. This section, combined with an understanding and assessment of the controls involved in the customers' business processes, aims to assist the customers' auditors to plan the audit of the financial statements and to assess the risk of misstatements in the customers' financial statements that may be affected by controls performed by IT Relation A/S.

Our testing of IT Relation A/S' controls only includes the control objectives and related controls referred to in the test table below. It does not include any of the controls that may appear from Management's description of the system. In addition, controls performed at the premises of IT Relation A/S' customers are not covered by our report. It is assumed that the latter controls are examined and assessed by the customers' own auditors.

Finally, the customers may have established compensating controls that help to minimize the control weaknesses referred to in this report to a level acceptable for audit purposes. Such assessment can only be made by the customers' auditors.

4.2 Control environment elements

This report is submitted using the partial method and does not cover controls that are carried out by sub-service organization EnergiMidt. Our testing of the control environment involved making inquiries of relevant members of management, supervisors and employees as well as examining IT Relation A/S' documents and recordings. The control environment has been assessed in order to determine the nature, timing and scope of the effectiveness of controls.

4.3 Test of effectiveness

Our test of the effectiveness of controls includes the tests we consider necessary to evaluate whether the controls performed and the observance of these controls are sufficient to provide a firm, but not an absolute, conviction that the control objectives specified has been achieved in the period from 01.10.2014 to 30.09.2015. Our test of the effectiveness of controls is designed to cover a representative number of transactions during the period from 01.10.2014 to 30.09.2015 for any control, see below, designed to achieve the specific control objectives. When selecting specific tests, we considered (a) the nature of the areas tested, (b) the types of available documentation, (c) the nature of audit ob-

jectives to be achieved, (d) the assessed control risk level and (e) the estimated effectiveness of the test.

4.4 Control objectives and control activities

The table below states the control objectives and controls tested. It also states the audit procedures performed and the results thereof. Where we have identified material control weaknesses, the table states so.

4.4.1 Internal organization of IT security

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
4.4.1.1 *Written guidelines & procedures*	An IT security policy has been drawn up and is reviewed at least once a year.	Deloitte has reviewed the most recently updated IT security policy and assessed whether the policy is implemented.	No comments.
4.4.1.2 *IT Risk analysis*	IT Relation A/S has prepared an IT risk analysis for critical systems applied in day-to-day operations. An annual assessment is made to establish whether procedures relating to risks and threats still apply, or the risk analysis needs to be changed.	Deloitte has assessed the most recently updated IT risk document and assessed whether approvals and mitigating factors were identified.	No comments.

4.4.2 Management of communication with customers

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: There is adequate user support for users who contact ServiceDesk, and the support agreed upon is provided within the area and time agreed upon.			
4.4.3.1 *Handling of incidents*	All customer inquiries are recorded as a case either in Efecte or in ITR-TID. The inquiries are prioritized and assigned to the persons who are to handle the case. The case development and the solution are documented in Efecte or ITR-TID. A continuous follow-up is performed to ensure that all cases are treated correctly.	Deloitte has assessed the procedures used and the controls performed. Deloitte has examined a sample of incidents received and observed that these are correctly followed up on and that this is documented in Efecte and ITR-TID.	No comments.

4.4.3 Backup

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: A security copy of data is made and stored so the data can be restored if lost. IT Relation A/S checks whether the backup is performed without any errors, and in case of errors in the backup that assessment and follow up of any errors are made.			
4.4.4.1 *Backup - strategy*	Backup strategies are prepared based on the SLA for the individual customers. Backup copies are made of all customer data and servers unless otherwise agreed with the customer.	Deloitte has examined the backup procedure and assessed whether it is sufficient to cover the backup requirements for critical systems and data as stated in the outsourcing agreements with the customers.	No comments.
4.4.4.2 *Backup - configuration*	IT Relation A/S uses a default backup configuration, which is used to make a backup of all customer data.	Deloitte has examined the backup configuration procedures and assessed the design of the control. Deloitte has made a random sample test of the backup configuration and compared it to the backup description prepared.	No comments.
4.4.4.3 *Backup – external storage*	External backup procedures have been performed at IT Relation A/S' location. These data are transferred to the primary center, EnergiMidt, which is located approx. 20 km from the location. Backup data are moved to a fire safe.	Deloitte has assessed the procedures used and the controls performed. Deloitte has ensured that the external storage of backup media is performed.	No comments.
4.4.4.4 *Backup - test*	Restore tests are made at regular intervals. Once a year, the backup is tested for restore of a customer's environment.	Deloitte has examined procedures for restoring files and full restore tests on the basis of backups. Deloitte has examined the latest backup tests for restoring a customer's environment from the backup.	No comments.

4.4.4 Operation and monitoring

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: It is monitored proactively that agreed-upon services are available, that available resources are in accordance with the agreed standard/threshold values and that necessary jobs and runs, online as well as batches, are performed correctly and in due time. IT Relation A/S checks that this is performed and with the expected result.			
4.4.5.1 *Batch and operation – written procedures*	IT Relation A/S uses established procedures in day-to-day operations and prepares control lists to document the operating controls performed.	Deloitte has assessed the operating procedures used and the controls performed. We have examined checklists by random sampling and examined whether the controls performed have been signed and that any misstatements observed have been handled.	No comments.
4.4.5.2 *Monitoring of operations – in general*	A procedure for automatically monitoring all servers and services is in place, and emails are sent to operating employees, notifying them of any alarms in the event of errors.	Deloitte has assessed the procedures used and the controls performed. Deloitte has examined the sample of alarms activated in the control environment and checked through their documentation that they have been followed up on.	No comments.
4.4.5.3 *Monitoring of capacity*	Alarms have been installed on hardware and all significant services (internal as well as customer services). All alarms are followed up on using real-time monitoring on screens located in the operations center.	Deloitte has assessed the procedures used and the controls performed. Deloitte has examined the monitoring of the operating environment by random sampling and checked that capacity management is set up for customers' systems.	No comments.

4.4.5 Access control

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: Access to systems, data and other IT resources is managed, maintained and monitored consistently with customers' requirements.			
4.4.6.1 *User rights – creation and changes*	Users are only created on basis of completed forms, which are sent to ServiceDesk. All creations are documented in Efecte. The users are granted rights according to customers' inquiries stated in the creation form.	Deloitte has assessed the procedures used and the controls performed. Deloitte has reviewed the documentation for user creation on a sample basis and assessed whether access and rights have been granted on a valid basis.	No comments.
4.4.6.2 *User rights – additional rights*	Internal employees' access to systems follows the same procedures as other users. Only a few key employees have been granted additional rights to the systems. Access to customer systems by IT Relation A/S' employees is logged.	Deloitte has assessed the procedures used and the controls performed. Deloitte has examined users holding additional rights within IT Relation A/S' main infrastructure, verifying that the rights have been granted upon approval.	No comments.
4.4.6.3 *User rights – deactivation*	Users are only terminated based on completed forms, which are sent to ServiceDesk. All terminations are documented in Efecte. It is the customers' own responsibility to inform about termination of users.	Deloitte has assessed the procedures used and the controls performed. Deloitte has made a random sample test on terminated users.	No comments.
4.4.6.4 *User rights – periodic reassessment of rights and deactivation*	Internal users of IT Relation A/S' management systems are regularly reviewed.	Deloitte has assessed the procedures used and the controls performed. Deloitte has reviewed the users of the internal management system.	No comments.

Control activity	Client control activity	Audit procedures performed	Test result
4.4.6.5 *IT security logging*	Logging of security incidents in IT Relation A/S' infrastructure has been set up. The logs are reviewed on a quarterly basis.	Deloitte has assessed the procedures used and the controls performed. Deloitte has verified whether the logging of critical systems and networks meets adopted logging requirements and whether logs are reviewed on a regular basis.	No comments.
4.4.6.6 *IT security organization*	IT security-related roles and responsibilities have been delegated, and employees are aware of their duties and functions.	Deloitte has reviewed the functions at the organization through interviews and verified through interviews with the employees that these match the actual roles and responsibilities.	No comments.
4.4.6.7 *Application of passwords.*	Users are authenticated through Windows AD, and access is managed from this environment in order to administer other parts of the infrastructure.	Deloitte has reviewed the configuration of password settings for critical internal systems, verifying that relevant users apply these.	No comments.
4.4.6.8 *Application of user profiles*	User accounts are created in Windows AD, and everyone applies individual user profiles on the internal network.	Deloitte has reviewed the application of user profiles on relevant systems and platforms, verifying that these are both personal and identifiable.	No comments.

4.4.6 Acquisition and maintenance of infrastructure

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: Network and communication software is maintained and supported, and management ensures that changes or new acquisitions are made as required and that changes are tested and documented satisfactorily.			
4.4.7.1 *Network and communication – patch management*	Relevant firmware upgrading is assessed and implemented regularly according to requirements. Firmware for network components is not changed unless security holes are observed.	Deloitte has assessed the procedures used and controls performed. We have assessed the design of controls and assessed that these are adequate. Furthermore, we have assessed the firewall change documentation and noted that all changes are automatically logged.	No comments.
4.4.7.2 *Network and communication - test*	Changes are tested on redundant equipment or less critical components before changes are implemented in production.	Deloitte has assessed the procedures used and the controls performed.	No comments.
4.4.7.3 *Network and communication - fallback*	Versioning tools are used for configuration of files for critical network components. Critical changes to network components are saved automatically in several versions so it will be possible to roll back to a previous configuration.	Deloitte has assessed the procedures used and controls performed for securing running and configurations on active network equipment.	No comments.
4.4.7.4 *Network and communication - timing*	Changes in network structures are most often made in defined service windows agreed upon with the customers.	Deloitte has assessed the procedures used and controls performed.	No comments.

Control activity	Client control activity	Audit procedures performed	Test result
4.4.7.5 *Network and communication – documentation of network*	The network is documented in different topology drawings and documents with information about IP addresses and VLAN configuration etc. Changes to the documentation are made in connection with creation of new customers in the hosted environment.	Deloitte has assessed the procedures used and controls performed. Deloitte has reviewed the latest network documentation and verified that this is regularly updated.	No comments.
4.4.7.6 *System software – patch management*	Windows platforms are continuously upgraded. The upgrades are obtained from Microsoft and managed through Lumension Endpoint Management.	Deloitte has assessed the procedures used and the controls performed. Deloitte has checked on a sample basis that servers are patched regularly.	No comments.
4.4.7.7 *System software – test.*	Tests are run by Lumension, who IT Relation A/S regards as competent for testing and assessing changes in system software.	Deloitte has assessed the procedures used and controls performed. Deloitte has assessed the documentation for the tests of changes to system software performed by Lumension.	No comments.
4.4.7.8 *System software – fallback*	Fallback for patching is to uninstall patches to the extent possible. If required, it is possible to restore from backup.	Deloitte has checked, on a sample basis, whether there has been a need for fallback in relation to patching, and if so, whether fallback could be completed.	No comments.
4.4.7.9 *System software – timing*	New upgrades are normally installed within the predefined service windows. The customers are warned about extraordinary service windows.	Deloitte has checked, on a sample basis, whether the timing of implementation at production level has been considered for the patching of system software.	No comments.
4.4.7.10 *System software – documentation of systems*	System software has been extensively documented for internal servers and the hosted environment.	Deloitte has checked whether the documentation of system software applied is adequate.	No comments.

4.4.7 Business continuity management

Control activity	Client control activity	Audit procedures performed	Test result
Control Objective: Ensure that an emergency plan is present and updated.			
4.4.8.1 *Business continuity management – Emergency plan*	IT Relation A/S has defined an emergency plan so that the company's internal IT applications can continue to run in case of an emergency.	Deloitte has assessed procedures used and controls performed. We have reviewed whether emergency plan for internal systems is available and updated on a regularly basis.	No comments.