www.pwc.dk

IT Relation A/S

Independent service auditor's assurance report on IT General Controls relating to financial reporting regarding IT Relation A/S' and IT Relation Philippines Inc.'s hosting services

January 2020

Contents

1 Service organisation's statement

The accompanying description has been prepared for customers who have used IT Relation A/S' hosting services and the customers' auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by the customers themselves, when assessing the risks of material misstatements in the customers' financial statements. IT Relation confirms that:

(a) The accompanying description in section 2 fairly presents the IT General Controls in relation to hosting services for customers throughout the period 1 January 2019 to 31 December 2019. The criteria used in making this assertion were that the accompanying description:

(i) Presents how the customers' solutions were designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed
- 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 those 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 during the period 1 January 2019 to 31 December 2019

(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 January 2019 to 31 December 2019. The criteria used in making this assertion 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 individuals who have the appropriate competence and authority, throughout the period 1 January 2019 to 31 December 2019.

Herning, 22 January 2020

Henrik Kastbjerg
CEO

2 *Description of IT General Controls at IT Relation A/S in relation to financial reporting for our hosting services*

Introduction to IT Relation A/S

IT Relation A/S[1] is an IT company focusing on optimising your business with IT solutions. We are specialists in IT strategy, hosting, security, support, hardware and development. Our 460 employees are split between eight locations across Denmark with offices in Herning, Aarhus, Copenhagen, Silkeborg, Kolding and Aalborg. In addition to the Danish locations, we have a location in the Philippines where selected tasks are performed for the customers who have approved this.

IT Relation is based on four business areas:

1. Managed Services (IT Outsourcing and Hosting)
2. Solutions (SharePoint, CRM, BI, Development, etc.)
3. IT Security
4. Hardware.

We strive to be a total end-to-end supplier of IT solutions through a 360-degree approach. Our 24/7 service desk is staffed with competent, flexible and smiling IT troubleshooters around the clock, 365 days a year. Our ambition for every single day is to deliver optimal IT solutions and ultimate customer service.

The “No Problem” culture

“No Problem” is the essence of IT Relation’s unique company culture. It is a unique approach when solving IT tasks for our customers and a set of values that we all focus on every day. It sets a clear direction for our behaviour when we aim to be **every day IT Superheroes** who:

- Say yes with a smile
- Understand the customer's business
- Think like a leader
- Make our colleagues better
- Make IT simple
- Keep our promises.

We believe that IT outsourcing deals with more than server capacity and new technology. It is about identifying areas where IT can support your growth potential and customise an IT solution that matches your ambition.

We promise you to:

- Remove your IT problems
- Improve your bottom line
- Smile while doing it.

2.1 Service statement introduction

This description has been prepared with the purpose of providing information to be used by IT Relation’s customers and their auditors, in accordance with the requirements of the Danish Standard on Assurance Engagements regarding controls within a service organisation: ISAE 3402. The description contains information about the system and control environment that has been established within IT Relation’s operating and hosting services rendered to their customers.

[1] Hereinafter referred to as IT Relation

This document comprises descriptions of the procedures used to safeguard the satisfactory operation of systems. The purpose is to provide sufficient information, so the hosting customers' auditors are able to independently assess the identification of risks of control weaknesses in the control environment, as far as this may involve a risk of material misstatement in hosting customers' IT operations for the period from 1 January 2019 to 31 December 2019.

2.2 Description of IT Relation's Services

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

IT Relation offers the following services to the hosting market:

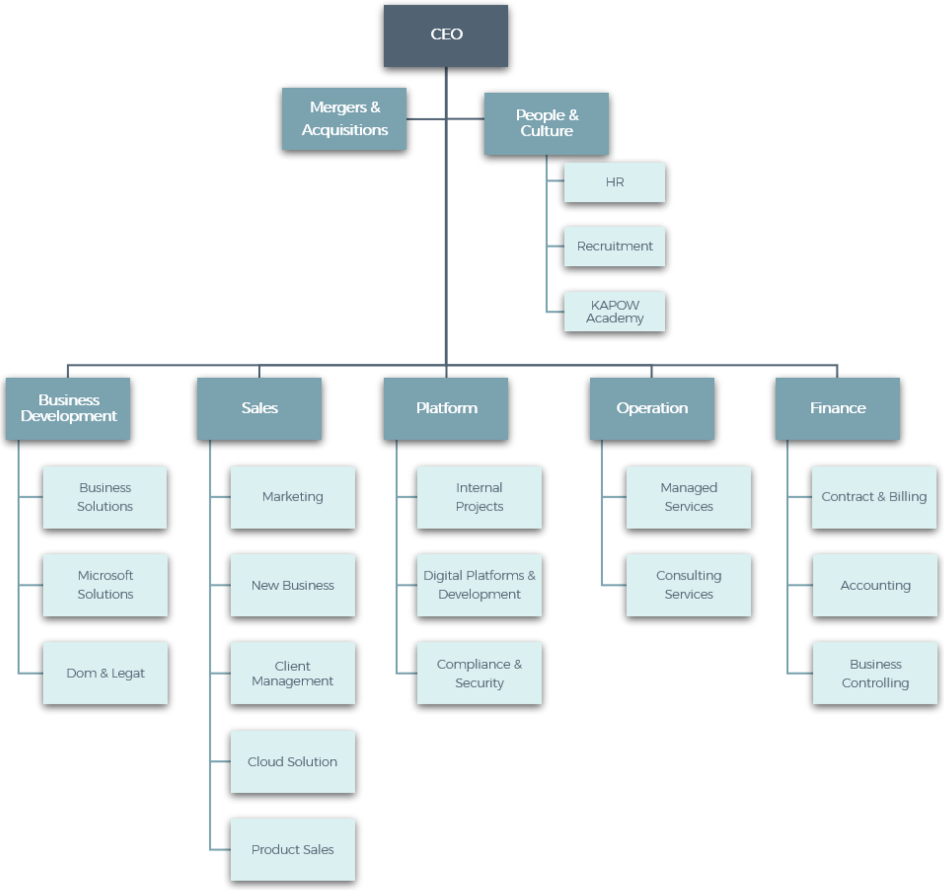
- Hosting and housing
- Remote backup
- Operation
- Cloud solutions
- Service desk.

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

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

- IT solutions development
- IT security advisory and services on both management and technical levels
- Advisory services at CIO level
- Technical project management
- On-site technical service.

2.3 The IT Relation organisation



2.4 Risk Management at IT Relation

Risk management at IT Relation is performed on several areas and levels. Once a year, risk and threat assessments are carried out aimed at internal systems in general. The input to this assessment is collected from the whole organisation. The process is facilitated by the Security Department that also prepares drafts for the management at IT Relation. After the internal processing, the assessment is approved by the management at IT Relation.

During 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 the operational project level, a continuous 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. The project manager will often choose to include project participants, external partners, and, if relevant, a steering committee, in the process.

2.5 Control framework, control structure and criteria for control implementation

The IT Security Policy, established processes and controls at IT Relation comprise all systems and services provided to customers. The continued work by adjusting and improving security measures is currently performed in cooperation with highly qualified specialists.

IT Relation is also subject to an annual system IT audit, which results in an annual auditor's report prepared in compliance with the ISAE 3402 standard. The decisions of criteria for control implementation at IT Relation are based on ISO 27001:2017.

Based on this control framework, control areas and control activities have been implemented according to best practice to minimise the risk of services provided by IT Relation. Based on the control model chosen, the following control areas are included in the overall control environment:

- Information security policies
- Organisation of information security
- Access control
- Physical and environmental security
- Human resource security
- Operations security
- Systems acquisition, development, and maintenance
- Information security incident management
- Information security aspects of business continuity management.

Each of the nine areas is described in detail in the sections below.

Information security policies	
Objective	A management-approved IT security policy has been prepared based on an IT risk analysis and communicated to relevant employees in the company.
Procedures and controls	IT Relation identifies relevant IT risks to which the services established are subject. This is handled through a current threat and risk assessment at IT Relation, partly in connection with all development projects and changes in system environments, and partly at an annual reassessment of the risk analysis. The result of the annual review is presented to the management. IT Relation also provides the hosting customers' auditors with information for their assessment of IT Relation as a service organisation. In addition to matters relating to operations, IT Relation 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.

Organisation of information security	
Objective	To manage information security within the organisation.
Procedures and controls	The primary responsibility for IT security lies with the executive board at IT Relation. This ensures that procedures and systems always support compliance with the current IT security policy. The Ministry of Security, in cooperation with Quality Management, 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 board has the following members: • Chief Technology Officer Anders Kaag • Head of Compliance and Security Frank Bech Jensen • Security Architect Kristian Brødløs • Team Leader Transitions Flemming Laursen • Cloud Citrix Specialist, Jakob Thalund Jensen • Team Manager Dan Sørup Olesen • Cloud Operation Specialist Jakob Andersen • Cloud Database Specialist Bo Duholm Hansen
Time of performing the control	The board meets once a year to determine and follow up on objectives in relation to IT security.
Who performs the control	The annual review is performed by the security board.
Control documentation	The board documents its decisions in an activity list.

Human resource security	
Objective	To ensure that employees and consultants understand their responsibilities and are suitable for their assigned roles. To ensure that employees and consultants are aware of and fulfil their responsibilities in relation to information security. To protect the organisation's interests as part of the process of changing or ending employment.
Procedures and controls	Part of the agreement with both permanent and temporary employees is to sign an employment contract and associated employment terms. A statement describes responsibilities and obligations regarding to IT security, and the terms include the current IT security policy and guidelines in addition to describing the secrecy and confidentiality statement. Criminal records are checked each year. Management must ensure that all employees implement and maintain IT security in accordance with the IT Relation IT Security Policy. The management responsibilities include the following for all employees: • They are adequately informed of their roles and responsibilities in terms of security before they are granted access to company systems and data. • They are familiar with the necessary guidelines so that they live up to the IT Relation IT Security Policy. • They are motivated to live up to the IT Relation IT Security Policy and achieve a level of attention in questions related to IT security that is consistent with their role and responsibilities in IT Relation. • They adhere to the guidelines and regulations for the recruitment, including the IT Relation IT Security Policy. • All employees in the organisation and, if applicable, consultants receive appropriate awareness training and regular updates in organisational policies and procedures relevant to their job function. Employees are continuously aware of and trained in the IT Relation IT Security Policy.
Retirement or termination	Responsibilities and obligations relating to information security, which remain valid after termination or amendment of employment conditions, are defined and communicated to the employee or the consultant – and enforced. When an employee resigns from IT Relation, the employee's direct manager is responsible for ensuring that all equipment is returned and that the retired access rights to information systems cease. Tasks and responsibilities in connection with termination of employment are described in the Retirement Policy. The purpose is to ensure that the resigned employee is aware and understands his/her responsibility after termination from IT Relation. At the end of the employment, it must be ensured that the resigned employee is informed of applicable IT security requirements and legal rules. The statement of silence continues after the resignation, and the resigned employee is expressly informed before the resignation.
Time of performing the control	At the time of employment and during our internal Kapow Academy training. At the time of resignation.
Control documentation	The HR department checks and files the contracts and checklists. At termination, the HR department checks and files the checklists. Agendas from info meetings regarding awareness. Certifications for specific technical skills.

Access control	
Objective	Access to systems, data and other IT resources is managed, maintained and monitored consistently in compliance with the customers' requirements. The access is divided into three areas: • Customer employees • IT Relation employees • Third-party consultants.
Procedures and controls	As a standard, a common system access is used for IT Relation 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 or requirements. Third-party consultants' accesses and rights to customer systems are only granted after a formal approval by the customer. Generally, users are created based on written inquiries sent to the operating department at IT Relation. IT Relation determines which of the pre-defined roles the users are to be assigned based on the customer's approval. Authorisation/rights for internal users at IT Relation are created according to the same principles as above 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 others, that a retired employee, when terminating his/her work at IT Relation, returns keys and access cards so no physical access to the building can be obtained and so the user ID cannot be used for log-in.
Time of performing the control	Customers: The control is performed when requested by the customer and when a third party accesses the customer's system. Employees at IT Relation: The control is performed in connection with changes in staff.
Who performs the control	Customers: The operating department of IT Relation is responsible for ensuring that the procedure for third-party access to the customer's environment is observed as agreed upon with the customer. Employees at IT Relation: The consultant and operations manager 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, the customer's IT manager will create an incident in the incident management system, detailing the scope of the third-party access. The operations department then formalises the access in an access agreement, which is sent back to the IT manager for acceptance and signature. The agreement is returned to the operations department that saves the agreement under the customer in IT Relation's document portal. For employees at IT Relation, the user forms are saved in the individual employee's staff file on the Executive Board drive.

Physical and environmental security

IT Relation has two primary data centres plus nine subsidiary data centres under decommissioning where IT equipment is placed. One location is in IT Relation's buildings in Viby. Nine data centres are at partner locations where IT Relation has an agreement regarding the physical security of these locations of the company's IT environments. The agreements are made with Eniig A/S, Nianet, Globalconnect and

NetCompany. IT Relation has full access to its customers' equipment placed at these housing partners. The internal data centres are fully operated by IT Relation.

Physical access control and security	
Objective	The physical access to systems, data and other IT resources is limited to and planned with the housing provider.
Procedures and controls	Access to the building is controlled through keys or electronic locking devices that have been handed over to IT Relation. Only people who need to have access to the server room in the housing centre has access to these keys. Finally, a key is required to get access to the rack cabinets used by IT Relation at external locations. The list of the keys handed out is kept and updated by the housing provider.
Time of performing the control	The list is validated once a year.
Who performs the control	The operating department and the housing provider perform the controls. Controls of handing out keys in general to the data centre are not part of this report.
Control documentation	The individual user of the key from IT Relation logs when collecting and returning keys to the housing centre records.

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 centre is protected against the following environmental incidents: • Power failure • Fire • Extreme climate conditions. In all vital IT equipment, a stable current is ensured by an UPS installation that provides the systems with electricity until the generator has automatically started. The technical room and the server room are provided with smoke and temperature sensors that are connected to the central fire surveillance system. The server room is also provided with automatic fire-fighting equipment (Inergen – activated in case of too high values of either smoke or heat). Fire protection equipment will automatically notify the fire department. The heat development in the server room is adjusted by the fully automatic cooling system, which ensures the correct temperature for stable operations and long durability of the IT equipment used. These plants are subject to continuous maintenance.
Time of performing the control	A daily visual control of the systems in the housing is performed by the housing provider.
Who performs the control	The control is performed by the housing provider. The Operations department performs the control of our internal data centre.
Control documentation	All control forms are located at the housing providers. For internal data centres, control is documented in control forms.

Operations security

Backup	
Objective	A security copy of data is made and stored in order to restore the data if lost. IT Relation checks whether a full backup has run. In case of errors, an assessment 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 system is physically placed in two different data centres. Backup data is then replicated from the primary to the secondary site on a daily basis to ensure an offline copy in case of a disaster.
Time of performing the control	Backup logs are checked during normal working hours.
Who performs the control	The Operations department handles the daily control of backup logs.
Control documentation	Daily operating check of the form and the annual check form.

Operations and monitoring	
Objective	Agreed-upon services are monitored proactively to ensure: • General availability • That available resources are in accordance with the agreed-upon standards and threshold values • That necessary jobs and batches are performed correctly and in due time. IT Relation makes sure that the above services follow the agreed-upon standards and that monitoring is performed with the expected result.
Procedures and controls	IT Relation has established a set of written procedures for all material operating activities supporting the general expectations for a satisfactory operation as stated in the IT Relation IT Security Policy. The operating procedures are prepared by the Operations department in close cooperation with the customer and third-party providers. Operations are handled through the platform tools of the Citrix servers. Several job descriptions for the Operations department define 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 immediately informed about the extent and the implications of the errors observed. The following functional areas have access to the customers' IT systems: • Service Desk employees • Operations employees • 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 the Operations department at IT Relation. The operations centre is monitored 24/7 at one or more of our locations in Herning and Viby, and, if the customers have agreed to it, the IT Relation location in the Philippines.
Control documentation	All incidents are logged in the monitoring system. Selected monitoring incidents are furthermore transferred to the IT Service Management system.

Patch management	
Objective	Patch management is performed based on the customer's agreement with IT Relation. The purpose is to ensure that systems are continuously updated with security patches to maintain a high level of security.
Procedures and controls	Contracts containing patch management means that IT Relation performs monthly patching with Microsoft updates as a standard. The patch routine is performed with a patch management system. IT Relation will approve patches for distribution every month immediately after Patch Tuesday. As a standard, all updates are approved. Only if a patch shows an issue, it will be excluded. Customer servers are updated as: • Automatic patch. The servers are configured in predefined service windows. Once the server reaches the service window, the client checks for approved updates and installs the missing updates. If updates cannot be installed within the service window, they will be pending and installed within the next service window. • Manual patch. The service window is configured at a specific time, and the patch routine is monitored. In addition, checks will be made after patching.
Time of performing the control	Controls are performed continuously through the patch management systems.
Who performs the control	Controls are performed by Operations.
Control documentation	All SCCM patches are automatically logged in individual log files at the specific server and site server. Manual controls are documented in the IT Service Management system.

Change management strategy	
Objective	Change management is performed with customers having an agreement that includes change management.
Procedures and controls	IT Relation has a change management procedure connected to customers having an agreement containing change management. The procedure includes: • Change Request (RFC) from the customer or from IT Relation • Clarification of terms and condition • Description of RFC execution, test, fall-back and risk • Approval process • Execution, test and fall-back if required • Documentation and RFC closing.
Time of performing the control	Controls are carried out during reporting to customers.
Who performs the control	Controls are performed by the Operations department at IT Relation. Outside normal working hours, the controls are performed by a consultant (back office).
Control documentation	Controls are documented in the Service Management System.

Logical access control – details

Registering users

All users are registered in one of the Active Directories that are part of the IT Relation Hosting environment. Administrative rights have been assigned to employees employed in IT Relation Operations. In addition, third-party Application Managers might have extended privileges on a specific server. In these cases, a third-party agreement has been established between IT Relation, the customer and the application provider.

Passwords

The user password must be complex, but at the same time possible for users to remember. Password policy is defined in the Employee - IT Security Policy.

Normal user AD passwords should be complex and with a minimum of 8 characters. Change is enforced after 90 days.

Password storage for the internal systems at IT Relation, including passwords giving full access to the individual Customer Hosted Servers, are stored in a closed encrypted asset management system. This can only be accessed with a personal login. Access to passwords in the asset management system is logged.

Periodic review of user access rights

Users with administrative rights are revised by changes in staff. Every 6 months there is also a manual review of the administrative users. This review is implemented by the Quality Manager.

Access to customer systems

Customer systems are accessed via specifically privileged jump-hosts to prevent access from other networks within or external to IT Relation.

System acquisition, development and maintenance

Network and communication software	
Objective	Network and communication software are maintained and supported. Management ensures that changes or new acquisitions are made as required and that changes are tested and documented satisfactorily.
Procedures and controls	IT Relation 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 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 any changes, 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 preparing upgrades and control of functionality.
Control documentation	Documentation of tasks performed in the customers system is managed in the IT service management system.

System software	
Objective	System software is maintained and supported. 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 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 patch management system. Thus, there is no manual assessment of these upgrades as the provider has tested and assessed the individual upgrades.
Time of performing the control	The control of upgrades is made through the patch management system, which contains logs for upgrades.
Who performs the control	Operations is responsible for preparing upgrades and the control thereof.
Control documentation	Apart from the documentation in the patch management system, logs are not made.

Information security incident management

Service desk and customer support	
Objective	That there is adequate user support for users who contact Service Desk and that the support agreed upon is provided within the agreed timeframe.
Procedures and controls	IT Relation has established a set of written service desk procedures in the areas agreed upon with the customer. The service desk procedures are prepared by Service Desk 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 prioritisations are made in the IT Service Management system.
Time of performing the control	Service Desk daily examines incidents that are waiting to be solved.
Who performs the control	Controls are performed by Service Desk 24/7 at the main office in Herning.
Control documentation	All incidents are logged in the IT Service Management system.

Incident handling	
Objective	Incident handling is performed satisfactorily based on the agreements made with customers, and IT Relation checks that this is made in full compliance with the agreement and with the expected result.
Procedures and controls	IT Relation uses an IT Service Management system to record and handle incidents. The following is recorded: • Errors (from e-mail or manually created records) • 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 Operations department is responsible for monitoring that inquiries targeted to Service Desk are prioritised and resources allocated – 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 Service Desk or Operations. Outside normal working hours, the incidents are handled by Service Desk and on-call consultants.
Control documentation	All incidents are logged in the IT Service Management system. There is no automatic escalation etc. in the IT Service Management system to check the compliance with SLA agreements. The customers themselves have access to follow cases in the ”Self Service Portal”.

Information security aspects of 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 has defined an operation emergency plan in order to make sure that the company’s internal IT applications can continue in case of an emergency. Furthermore, there is a defined cyber-attack emergency plan to make sure that attacks are handled effectively. Plans are reviewed on a regular basis.
Time of performing the control	The control of upgrades and test of emergency plans are performed annually.
Who performs the control	The Operations department is responsible for preparing upgrades and the control thereof.
Control documentation	Review of emergency plans and test of procedures are documented when performed.

Contingency plans

IT Relation is very dependent on functioning internal IT systems. We are therefore prepared to ensure rapid reestablishment of critical systems in case of a severe crash.

Vital systems that will be restarted within 24 hours include:

- Hyper-V environment
- VMWare environment
- ISP lines
- Firewall
- Internal infrastructure
- IT Relation A/S servers (DC – SQL – asset management system – Citrix)
- IT Relation A/S Backup systems (TSM)
- Telephony
- Customers of IT-Relation A/S operations.

The IT emergency plan is prepared and maintained based on ongoing risk analysis of the company's IT environment.

The risk analyses reveal the individual units' dependence on the different IT systems and services so that management requirements for availability are met and reflected in contingency planning to the greatest extent possible.

Situation management

A technician at IT Relation becomes aware of a serious operating incident. The extent of the problem is diagnosed and if the event is categorised as priority 1, situation management will begin immediately.

The error is escalated personally or by telephone to the available situation manager.

The situation management then continues after specified procedures to identify the extent of the problem, ensure adequate staffing, plan, involve external staff, resolve the issue, collect periodic status, ensure information to customers, etc.

After solving the issue and performing relevant and specified controls, the situation management is closed. Within a short time, the incident is analysed and evaluated to conclude if further actions are necessary.

Emergency operation

Emergency server operation is defined as the prioritisation of high-priority applications and services using systems with limited capacity (server operation) in an accident or disaster situation. Emergency operations can be established from either primary or secondary locations.

Emergency service desk operations are defined as the prioritisation of high-priority tasks performed by employees at IT Relation using systems with limited capacity in an accident or disaster situation. Emergency operations can be established from either primary or secondary locations and service desk home workplaces until premises can be rented and external lines established.

2.6 Additional information on the control environment

Matters to be considered by the customers' auditors

Services provided

The above system description of controls is based on the IT Relation standard terms. Consequently, the customers' deviations from the IT Relation 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 that are relevant for the presentation of the customers' financial statements.

User administration

IT Relation grants access and rights in accordance with customer instructions when these are reported to Service Desk. IT Relation 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 also provides access to third-party consultants, primarily developers who are to maintain applications being part of the hosting agreement. This is performed according to instructions from the IT Relation 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 do not define any requirements of emergency planning and restoring of the customers' system environment in case of an emergency.

IT Relation 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 hosting 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 has planned procedures and controls so that legislation in the areas for which IT Relation is responsible is adequately observed. IT Relation is not responsible for applications that run on the hosted equipment. Consequently, this report does not extend to assure 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 legislations.

3 Independent service auditor's assurance report on the description, design and operating effectiveness of controls

TO the Management of IT Relation A/S, IT Relation A/S' customers of hosting services in the period 1 January 2019 to 31 December 2019 and their auditors

Scope

We have been engaged to report on IT Relation A/S' description in section 2 of IT General Controls related to financial reporting for hosting services (processing customers' transactions) related to general agreements between IT Relation A/S and IT Relation A/S' customers throughout the period 1 January 2019 to 31 December 2019 (the description) and the design and operation of controls related to the control objectives stated in the description at physical locations in Denmark.

IT Relation A/S' responsibilities

IT Relation A/S is responsible for: preparing the description and accompanying statement in section 1, including for the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR – danske revisorer, which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

PricewaterhouseCoopers 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.

Service auditor's responsibilities

Our responsibility is to express an opinion on IT Relation A/S' description and on the design and operation of controls related to the control objectives stated in the description, based on our procedures. We have conducted our assurance engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board. This standard requires that we plan and perform our work to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of 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 considered 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 and described in section 1.

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

IT Relation A/S' description has been prepared to meet the common needs of its customers and their auditors and may not, therefore, include every aspect of IT General Controls that every single 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. Furthermore, 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 are those described in section 1. In our opinion, in all material aspects:

a) The description fairly presents the operational services as designed and implemented at physical locations in Denmark throughout the period 1 January 2019 to 31 December 2019

b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 January 2019 to 31 December 2019

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives were achieved, operated effectively throughout the period 1 January 2019 to 31 December 2019.

Please note that our opinion alone covers operational services related to general agreements between IT Relation A/S and IT Relation A/S' customers; customer-specific requirements and other matters are not included. In so far as a customer requests a statement on such requirements and matters, said customer must enter into a separate agreement with IT Relation A/S.

We furthermore believe that the system and data integrity, availability and confidentiality can be considered satisfactory for the period.

Description of tests of controls

The specific controls tested and the nature, timing and results of these tests are listed in section 4.

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used IT Relation A/S' hosting services and their auditors who have a sufficient understanding to consider these, along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatements in customers' financial statements in the period 1 January 2019 to 31 December 2019.

Aarhus, 28 January 2020
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper P. M

Jesper Parsberg Madsen
State-Authorised Public Accountant

Iraj Bastar
Senior Manager

4 Control objectives, controls, tests and related findings

Control objective A: Information security policy

Management has prepared a security policy that outlines clear IT security objectives, including choice of framework and resource allocation. The information security policy is maintained with due consideration of an up-to-date risk assessment.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Written information security policy The information security policy is documented, audited and updated as required at least once a year. The information security policy is approved by Management. The information security policy is made available to employees via the intranet.	We have made enquiries of Management about the overall management of information security and investigated whether Management has approved the security policy and whether the policy is subject to audit at least once a year.	No exceptions noted.

Control objective B: Organisation of information security

The organisational responsibility for information security is properly documented and established. Relationships with external parties are managed through agreements providing sufficient security.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Management's information security-related responsibility The organisational responsibility for information security is documented and implemented. In addition, rules for confidentiality agreements have been established, as has the reporting on information security incidents.	We have made enquiries of Management about the overall management of information security and investigated whether an efficient security organisation exists supporting IT Relation A/S' business areas.	No exceptions noted.
External parties Identification of risks related to external parties, including addressing security in third-party agreements and security issues related to customers. Identified control weaknesses are also audited. Issues are investigated and resolved in a timely manner.	We have made enquiries of Management about the procedures/control activities performed and investigated whether the necessary security has been established in agreements with third parties, including that IT Relation A/S' security standard is observed and that, where relevant, assurance statements are obtained from significant external suppliers. By inspection, we have observed that agreements have been signed with external parties.	No exceptions noted.

Control objective C: Physical security

Operations are undertaken at locations that are protected from damage resulting from e.g. fire, water leaks, power outage, theft or vandalism.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Physical security – delimitation of boundaries Access to secured areas (for new as well as existing employees) is limited (e.g. by using access cards) to authorised employees and is based on documented management approval. Currently, the secured access areas consist of the following three zones and the criteria are as described. Deviations from the criteria described for each zone require approval by the managing director. Zone 1: Office areas. All employees in IT can get an approval. Zone 2: Hosting and production areas. Requires employment relationships in the technical part of IT Relation. Zone 3: Data site. Requires hiring in the technical part of IT Relation and backup-related work tasks. Persons without approval to secured zone 2 areas must be registered and accompanied by an employee with sufficient level of approval.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, tested whether: • the physical area is divided into three zones • access to IT Relation A/S' locations is limited to authorised employees, including through personal ID cards • a procedure exists for escorting of visitors from the front desk • access to server rooms is limited for technicians only and is based on two-factor authentication.	No exceptions noted.
Securing offices and other facilities An access control system has been set up for all server rooms ensuring that access is restricted to employees with the appropriate Management authorisation. According to the "Physical Security" item, accesses in connection with changes in employment conditions or assignments regarding access rights are revised at least once a year.	We have made enquiries of Management about the procedures/control activities performed and investigated whether an electronic system has been established to grant and register access to systems placed in IT Relation A/S' operational facilities. Using random samples, we have moreover tested whether periodic audit of granted access rights is performed.	No exceptions noted.

Control objective C: Physical security

Operations are undertaken at locations that are protected from damage resulting from e.g. fire, water leaks, power outage, theft or vandalism.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Positioning and securing of equipment The data centre is protected against physical conditions such as fire, water and heat. Equipment for monitoring the indoor climate, including humidity, has furthermore been installed.	We have made enquiries of Management about the procedures/control activities performed, paid a visit to IT Relation A/S' operational facilities and investigated whether necessary control measures suitable for data centres have been established, i.e.: • fire prevention measures • measures to prevent moisture • cooling measures. During our audit, we have furthermore investigated whether monitoring has been established with respect to operational facilities.	No exceptions noted.
Supporting power supply equipment (supply security) The data centre is protected against interruptions to the power supply with the help of UPS (uninterruptible power supply) or emergency power system. Data centres are protected from power interruption using uninterruptible power supply (UPS) and diesel-powered emergency power plants. Start test and "live test" are being executed quarterly with full load on UPS and diesel generator, respectively. In addition, the equipment is covered by service agreements with suppliers. Fire extinguishing equipment is tested by the supplier under the applicable service agreements.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, investigated whether suitable redundancy has been established for those of IT Relation A/S' systems that relate to the company's hosting services. Using random samples, we have observed that service reports for equipment exist.	No exceptions noted.

Control objective C: Physical security

Operations are undertaken at locations that are protected from damage resulting from e.g. fire, water leaks, power outage, theft or vandalism.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Secure wiring All network cables are properly installed and are located at a data site. Guest access is only available through WiFi and is exclusively available in separate guest zones.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, tested whether: • access to IT Relation A/S' locations is limited to authorised employees, including through personal ID cards, as stated in the rules for securing offices and other facilities • wiring critical to operations is buried or adequately protected through other means. By inspection, we have also observed that guests have only access through guest WiFi.	No exceptions noted.

Control objective D: Communications and operations management

The below have been established:

- *Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents*
- *Sufficient procedures for backup and contingency plans*
- *Appropriate segregation of duties in and around IT functions, including between development, operations and user functions*
- *Appropriate business processes and controls pertaining to data communication that seek to prevent loss of authenticity, integrity, availability and confidentiality.*

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Documented operating procedures Operation manuals and implementation procedures for all essential IT areas have been described. Each IT area is responsible for maintenance of existing manuals and procedures.	We have made enquiries of Management about the procedures/control activities performed and investigated whether suitable operating documentation has been established. By inspection, we have observed that there are documented operating procedures and that a connection exists between the documentation and the actions actually performed.	No exceptions noted.
Segregation of duties Management has implemented policies and procedures to ensure satisfactory functional segregation in the IT department. These policies and procedures include requests that: • Access is authorised based on a work-related need • IT Relation's administrative platform is separate from the technical platform regarding network- and user-access • Access to the hosting environment is granted only to employees with authorised and sufficient approval.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, investigated whether suitable segregation of duties has been established between critical operating functions in IT Relation A/S and between technical and administrative platforms.	No exceptions noted.
Measures to protect against virus and similar malicious code Anti-virus programs have been installed, and these are updated regularly.	We have made enquiries of Management about the procedures/control activities performed and investigated whether anti-virus measures have been implemented protecting adequately against spam, virus and other malicious code.	No exceptions noted.

Control objective D: Communications and operations management

The below have been established:

- *Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents*
- *Sufficient procedures for backup and contingency plans*
- *Appropriate segregation of duties in and around IT functions, including between development, operations and user functions*
- *Appropriate business processes and controls pertaining to data communication that seek to prevent loss of authenticity, integrity, availability and confidentiality.*

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Backup of information Backup of data is performed at appropriate intervals. Periodically, a test is performed to verify that data can be recovered from backups. As a backup system internally as well as hosting solutions, IT Relation uses remote backing products following the same SLA as external customers. For hosted services, frequency and versions will be described and agreed in the individual contract, based on a minimum security period of four weeks. An additional copy of backup data is also made to a remote location.	We have made enquiries of Management about the procedures/control activities performed and investigated whether implemented controls work according to the following guidelines: • Backup is tested continually • Monitoring has been implemented to ensure that continual and correct backup is performed. We have tested whether procedures and controls work according to IT Relation A/S' security standards. Using random samples, we have observed that data from backup can be recovered.	No exceptions noted.
Monitoring of system use and audit logging Logging has been implemented on all critical systems. Logs from critical systems are being reviewed in case of suspected unauthorised events and activities. Critical activities and access from users with privileged rights (e.g. super users) will be logged in all IT Relation critical systems used for task management. Especially, critical operating systems and network transactions are being monitored. Deviations are investigated and resolved in a timely manner.	We have made enquiries of Management about the procedures/control activities performed, and, using random samples of technical set-ups, we have moreover investigated whether: • logging of critical transactions and use of privileged rights have been implemented • a process exists for timely follow-up on deviations.	No exceptions noted.

Control objective D: Communications and operations management

The below have been established:

- *Appropriate business processes and controls in relation to operations, including monitoring and registration of, as well as follow-up on, relevant incidents*
- *Sufficient procedures for backup and contingency plans*
- *Appropriate segregation of duties in and around IT functions, including between development, operations and user functions*
- *Appropriate business processes and controls pertaining to data communication that seek to prevent loss of authenticity, integrity, availability and confidentiality.*

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Error logging IT Relation A/S has established monitoring systems configured to detect errors in operating systems on the basis of predefined criteria. System-generated errors are examined and remediated within an acceptable timeframe based on their severity. Important alarms will be handled 24/7/365 via permanent on-site staffing or operating specialists on duty.	We have made enquiries of Management about the procedures/control activities performed, and, using random samples of the incident process, we have moreover investigated whether monitoring and registration of errors have been established in operating systems. Auditing the incident process, we have furthermore investigated whether errors are examined and remediated within an acceptable timeframe.	No exceptions noted.
Incident reporting IT Relation A/S has implemented rules and procedures to ensure that reporting on information security-related incidents takes place.	We have made enquiries of Management about the procedures/control activities performed and investigated whether procedures have been implemented for timely reporting of security-related incidents.	No exceptions noted.

Control objective E: Access control

The below have been established:

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data*
- *Logical and physical access controls reducing the risk of unauthorised access to systems and data*
- *Logical access controls supporting organisational segregation of duties.*

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
User registration and privilege administration All access to operating systems, networks, databases and data files made available to new and existing users is audited in order to ensure compliance with company policy. Steps are also taken to ensure that access permissions are dependent on the requirements of the job function and are approved and set up correctly in the systems.	We have made enquiries of Management about the procedures/control activities performed, audited user administration procedures and, using random samples, investigated whether: • according to guidelines, periodic follow-up is performed on users' rights in operating environments • the above rights are granted based on a work-related need.	We have observed that there is not sufficient documentation for the approval of the created user accounts for user accounts for all samples. We have been informed that a new process for approval of user accounts with administrator rights has been implemented in November 2019. We have received documentation that confirms effectiveness of the above mentioned new process. No further exceptions noted.
Administration of user access codes Access to operating systems, networks, databases and data files is password-protected. Password quality requirements have been set to require a minimum length (8 characters) and complexity and a maximum execution time (90 days), and the password settings do not allow passwords to be reused. Users are also locked out after a set number of failed login attempts. Critical systems are integrated with Windows Domain Controller. Furthermore, physical and logical access to network has been restricted.	We have made enquiries of Management about the procedures/control activities performed, and, using random samples of technical set-ups, we have moreover investigated whether: • passwords are used in accordance with guidelines • programmed controls ensure that passwords are changed regularly.	No exceptions noted.

Control objective E: Access control

The below have been established:

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data*
- *Logical and physical access controls reducing the risk of unauthorised access to systems and data*
- *Logical access controls supporting organisational segregation of duties.*

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Assessment of user access rights Management periodically audits user access permissions to ensure correspondence with the requirements of the users' job functions. Discrepancies are investigated and resolved in a timely manner.	We have made enquiries of Management about the procedures/control activities performed and investigated whether, in accordance with guidelines, periodic follow-up is performed on users' rights in operating environments and whether these rights are granted based on a work-related need.	No exceptions noted.
Revoking access rights User permissions granting access to operating systems, networks, databases and data files pertaining to employees who have left the company are revoked in a timely manner. Revoking of access rights will be initiated by approval from the users' manager.	We have made enquiries of Management about the procedures/control activities performed and investigated whether, in accordance with guidelines, periodic follow-up is performed on users' rights in operating environments and whether these rights are granted based on a work-related need.	No exceptions noted.
Policy on use of network services, including authentication of users with external connections Data communication has been suitably defined and is sufficiently protected against the risk of loss of authenticity, integrity, availability and confidentiality. Networks have also been divided where necessary or agreed with the customer. The division of network follows IT Relation's procedures for segregation of duties. VPN is offered from statics IP addresses and two-factor authentication (token) to certain parts of the technical platform. To the administrative platform, a token system is used. The mentioned platforms are separated by the implementation of several VLANs.	We have made enquiries of Management about the procedures/control activities performed, audited the technical architecture and, using random samples, investigated whether, in accordance with guidelines, a suitable security level has been established, including that: • The network is segregated in secure zones and customer environments are segregated from IT Relation A/S' own environment. • Two-factor authentication (token) is used as described.	No exceptions noted.

Control objective E: Access control

The below have been established:

- *Appropriate business processes and controls for granting, following up on and maintaining access rights to systems and data*
- *Logical and physical access controls reducing the risk of unauthorised access to systems and data*
- *Logical access controls supporting organisational segregation of duties.*

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Management of network connections IT Relation A/S manages network security through several control measures. Customers are provided with individual VLANs. Firewall ruleset is being reviewed periodically, and the traffic through firewall is being tested and monitored.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, investigated whether, according to guidelines, a suitable security architecture has been established in the network, including that: • the network is segregated in secure zones and that customer environments are segregated from IT Relation A/S' own environments • changes to the infrastructure, chosen for our random samples, are carried out in a controlled manner as described in the change management procedure.	No exceptions noted.
Restricted access to information All requests for access from new and existing users pertaining to applications, databases and data files are audited to ensure compliance with company policy in order to ensure that permissions are dependent on the requirements of the job function, have been authorised and are correctly set up in the systems.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, investigated whether, in the period and in accordance with guidelines, approval has been granted of access requests regarding access to applications, databases and data files. Using random samples, we have moreover audited selected systems and investigated whether access is granted based on a work-related need.	No exceptions noted.

Control objective F: Acquisition, development and maintenance of operating systems

Appropriate procedures and controls have been established for implementation and maintenance of operating systems.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Management of software on operational systems Separate IT environments for development, testing and production have been established. Only employees with separate functions can migrate changes between the individual environments.	We have made enquiries of Management about the procedures/control activities performed and, using random samples, investigated whether, in accordance with guidelines, separate environments have been established for development, testing and operation and whether suitable segregation of duties has been established in relation to operation of new functionality.	No exceptions noted.
Change management IT Relation has implemented change management procedures at two levels. Full Change Management is implemented on shared infrastructure and on Customer systems where Change Management procedure has been agreed. For systems and Customers not covered by the full Change Management procedure, changes are evaluated and recorded as a Service Requests. The formalised Change Management procedure for changes are applied to applications, operating systems and networks and changes are assessed and executed by qualified personnel and, if possible, tested on test systems before commissioning. Changes have a documented plan for implementation, fallback and test. If change is performed on a Customer system, the change is reconciled with the customer before execution. Pre-approved changes are standard changes that have been approved in advanced, e.g. frequent repetitive actions like patch management, etc. Emergency changes to operating systems and networks that are performed by bypassing the normal change management procedures will be tested and approved later. When Changes are recorded as Service Requests, execution is performed only in a service windows that are agreed with the customer. Documentation of Service	We have made enquiries of Management about the procedures/control activities performed and, using random samples from the system used for documenting changes, investigated whether, in accordance with guidelines, changes to the operating environment are carried out utilising a controlled process, including that: • an approved test is performed prior to changes being implemented • testing and approval of emergency changes to the operating environment are documented immediately following the changes being implemented • standard changes are preapproved • handling the changes is compliant with the approved change management procedures.	No exceptions noted.

Control objective F: Acquisition, development and maintenance of operating systems

Appropriate procedures and controls have been established for implementation and maintenance of operating systems.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Requests is done in IT Relation Service Management System.		

Control objective G: Disaster recovery

IT Relation A/S is able to continue servicing its customers in a disaster situation.

IT Relation A/S' control activity	Control tests performed by PwC	Results of PwC's tests
Structure of IT Relation A/S' disaster preparedness The combined disaster recovery and contingency plan comprises an overall disaster management procedure and operational disaster recovery and contingency plans for the specific disaster areas. The operational disaster recovery and contingency plan includes a description of the disaster organisation with management job descriptions, contact information, notification lists and instructions for the necessary task groups. Detailed task group instructions for restoration in connection with emergency operations have been prepared for the individual platforms.	We have made enquiries of Management about the procedures/control activities performed and investigated whether, in accordance with guidelines, a suitable disaster recovery plan has been prepared with respect to operations.	No exceptions noted.
Test of disaster recovery Once a year, IT Relation A/S audits the disaster recovery plan and performs tests via high-impact operating disturbances, such as breakdowns of central data centre infrastructure.	We have made enquiries of Management about the procedures/control activities performed and investigated whether, in accordance with guidelines, periodic tests are performed of the disaster recovery plan, whether possible disturbances are documented and whether remediation is included in the plan.	No exceptions noted.