www.pwc.dk

IT Relation A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2020 to 31 December 2020 in relation to IT Relation's hosting services

February 2021

Contents

1 Management's statement

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

IT Relation A/S uses Global Connect, Eniig, Sentia and InterXion as a subservice supplier for housing services. This report uses the carve-out method and does not comprise controls that Global Connect, Eniig, Sentia and InterXion perform for IT Relation A/S.

IT Relation A/S uses B4Restore and Front-Safe as a subservice supplier for backup services. This report uses the carve-out method and does not comprise controls that B4Restore and Front-Safe perform for IT Relation A/S.

IT Relation A/S confirms that:

a) The accompanying description in section 3 fairly presents the hosting services that have processed customers' transactions throughout the period from 1 January 2020 to 31 December 2020. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to hosting services were designed and implemented, including:

   - The types of services provided
   - The procedures, within both information technology and manual systems, by which the IT general controls were managed
   - Relevant control objectives and controls designed to achieve those objectives
   - Controls that we assumed, in the design of hosting services, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
   - How the system dealt with significant events and conditions other than transactions
   - 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 the IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to hosting services during the period from 1 January 2020 to 31 December 2020

   (iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to the hosting services 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 IT general controls in relation to hosting services that each individual customer may consider important in its own particular environment.

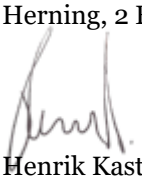
b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2020 to 31 December 2020. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2020 to 31 December 2020.

Herning, 2 February 2021



Henrik Kastbjerg

IT Relation A/S
Dalgas Plads 7B, 1 Floor
DK-7400 Herning

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2020 to 31 December 2020 in relation to IT Relation's hosting services

To: IT Relation A/S (IT Relation), IT Relation's customers and their auditors

Scope

We have been engaged to provide assurance about IT Relation's description in section 3 of its IT general controls in relation to hosting services which have processed customers' transaction throughout the period from 1 January 2020 to 31 December 2020 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

IT Relation uses Global Connect, Eniig, Sentia and InterXion as subservice suppliers for housing services. This report uses the carve-out method and does not comprise controls that Global Connect, Eniig, Sentia and InterXion perform for IT Relation.

IT Relation uses B4Restore and Front-Safe as a subservice supplier for backup services. This report uses the carve-out method and does not comprise controls that B4Restore and Front-Safe perform for IT Relation.

IT Relation's responsibilities

IT Relation is responsible for: preparing the description and accompanying statement in section 1, including 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.

Service auditor's independence and quality control

We have complied with the independence and other ethical requirements of the Code of Ethics for Professional Accountants issued by FSR – Danish Auditors, which are based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct.

PricewaterhouseCoopers is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and 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's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its hosting services 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 consider necessary to provide

reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by IT Relation in the Management's statement section.

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'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 hosting services that the individual customer may consider important in its particular circumstances. 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 auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

a) The description fairly presents how IT general controls in relation to hosting services were designed and implemented throughout the period from 1 January 2020 to 31 December 2020;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2020 to 31 December 2020; and

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2020 to 31 December 2020.

Description of test 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's hosting services and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Aarhus, 2 February 2021
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab

Jesper Parsberg Madsen
State-Authorised Public Accountant

Iraj Bastar
Director

3 IT Relation's description of IT general controls relating to financial reporting for IT Relation's 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 520 employees are split between five locations across Denmark with offices in Herning, Aarhus, Copenhagen, Kolding and Aalborg. In addition to the Danish locations, we have one 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 trouble-shooters 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 which 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
- Thinks like a leader
- Makes our colleagues better
- Makes IT simple
- Keeps 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.

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 2020 to 31 December 2020.

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:

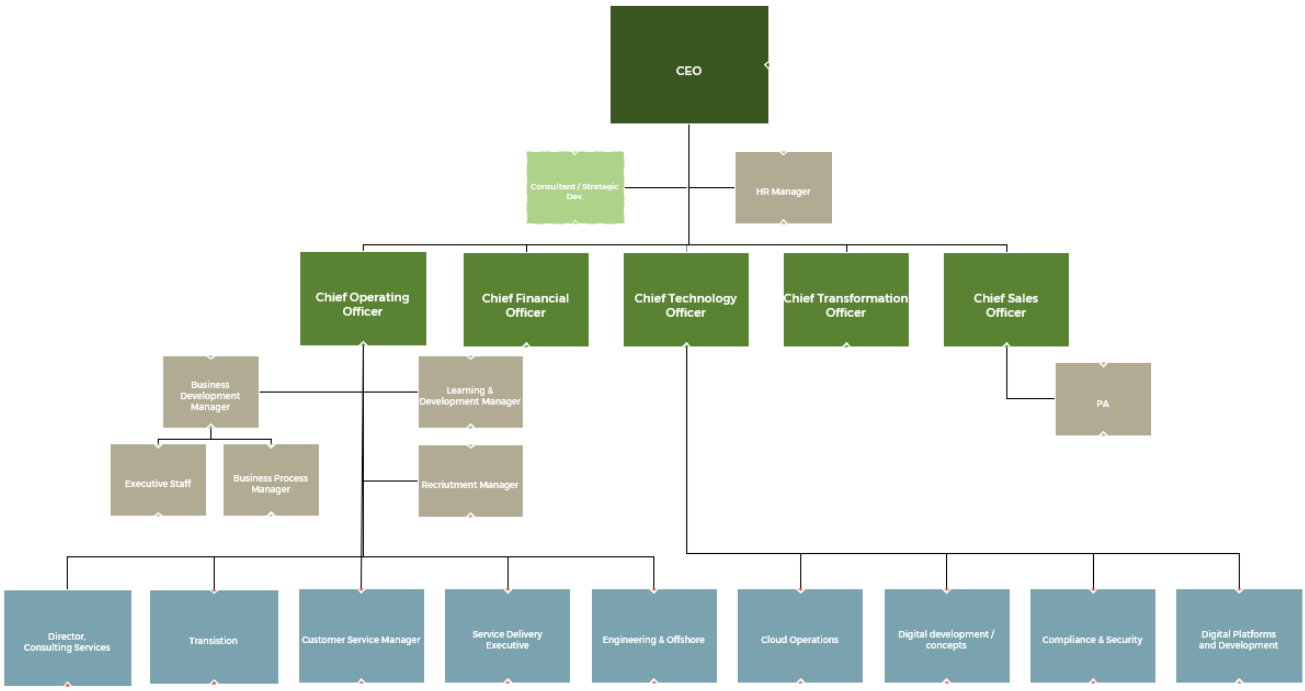
- Hosting and housing
- Remote backup
- Operation
- Cloud solutions
- Service Desk.

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.

The IT Relation organisation



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, which 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.

Control framework, control structure and criteria for control implementation

The IT Security Policy established processes, and controls at IT Relation, comprises 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 certified according to the ISO 27001: 2013 standard. This means that controls from the standard are implemented and complied with. As part of the ISO 27001 standard, a management system for information security (ISMS) has also been established.

With the management we are:

- Monitoring and measuring status of information security
- Performing internal audits
- Evaluating information security and measures
- Performing Management review with top management.

The purpose of ISMS is to ensure ongoing control of the level of information security in relation to the threat level in general. On the basis of ISMS, a continuous improvement process is maintained which ensures that incidents are processed and that the level of information security is continuously improved.

IT-Relation is also subject to an annual IT audit which results in an annual audit report prepared in compliance with the ISAE 3402 standard. Controls that have been implemented and revised are controls from Annex A in ISO 27001: 2013.

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
- Human resource security
- Access control
- Physical and environmental security
- Protection against environmental incidents
- Operations security
- Operations and monitoring
- Patch management
- Change management strategy
- Network and communication software

- System software
- Service desk and customer support
- Incident handling
- 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 • Cyber security manager, Kristian Brødløs • Team Leader Transitions, Flemming Laursen • Cloud Citrix Specialist, Jakob Thalund Jensen • Team Manager, Dan Sørup Olesen • Cloud Operation Specialist, Jakob Andersen • Compliance 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 their 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: • That they are adequately informed of their roles and responsibilities in terms of security before they are granted access to company systems and data. • That they have been made familiar with the necessary guidelines so that they can live up to the IT Relation IT Security Policy. • That 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 are consistent with their role and responsibilities in IT Relation. • That 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 is 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 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 is informed of applicable IT security requirements and legal rules. The confidentiality agreement continues after the resignation, and the resigned 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 are 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	Accounts that IT Relation uses on customer systems are often accounts with extended privileges. By default, IT Relation's employees' access to the customer's system is granted based on the employee's role. This includes that when the employee is in a job function that has a work-related need for access to customer systems, this access is granted. IT Relation's access to customer systems is logged. As an enhanced protection of IT Relations' access to customer systems, IT Relation offers a Just-in-Time solution. Just-in-Time is a system for protecting IT Relation's administrative accounts. This ensures that the use of access is logged and traceable, that strong passwords are used, and that passwords are automatically changed each time the account is used. With Just-in-Time, no one knows the password when IT Relation is not logged in. This limits the possibility that an IT Relation account can be used for lateral relocation of a hacker. Third-party consultants who must have access to the customer's platform are set up as local administrators of the specific systems that they need access to. Third-party consultants' access and rights to customer systems are granted only after a formal approval from the customer. In general, third-party users are created based on a written inquiry to the operation department in IT Relation. IT Relation determines which of the predefined roles users should be assigned based on customer approval.
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 are 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 that is sent back to the IT manager for acceptance and signature. The agreement is returned to the operations manager who saves the agreement under the customer in IT Relation's document portal under the customer. 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 Norlys A/S, Interxion, 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 which have been handed over to IT Relation. Only people who need access to the server room in the housing centre have 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 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 which 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 which are connected to the central fire surveillance system. The server room is also provided with automatic fire-fighting equipment (Inergen – which is activated in case of too high values of either smoke or heat). The 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 has 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 on shared infrastructure and customers' systems when the customer has an agreement that includes change management.
Procedures and controls	IT Relation has a change management procedure which is used when: • Changes are being made in shared infrastructure systems • Changes are being made to customers' systems on customers who have change management included in their contract. The procedure includes: • Change request (RFC) from the customer or from IT relationship • Clarification of terms and conditions • Description of RFC performance, test, fallback and risk • Approval process • Execution, test and fallback if required • Documentation and RFC closure. For customers without change management included, changes are made based on a service request in IT Relations' ITSM system.
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 which 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 eight 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 and copying of 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 six 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 for 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 which 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 incidents (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 cyberattack 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 well-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:

- HyperV 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
- Telephony
- Customers of IT-Relation A/S operations.

The IT emergency plan is prepared and maintained based on an 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, to the greatest extent possible, are met and reflected in the contingency planning.

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.

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, which are relevant for the presentation of the customers' financial statements. For change management, only the core infrastructure is covered by the standard contracts, and any change management on customer solutions is to be covered by a separate agreement with IT Relation.

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.

As a standard, a common system access is used for IT Relation and the customer's internal IT employees (common administrator password). The accounts used by IT Relation are often accounts with extended privileges. As an enhanced protection of these accounts, IT Relation offers a Just-in-Time solution. This is not part of standard contract with IT Relation. Just-in-Time is a system to protect IT Relation's administrative accounts. It ensures that the use of access is logged and is traceable, that strong passwords are used, and that passwords are changed every time the account has been used. With Just-in-Time, no-one knows the password when IT Relation is not logged in. This limits the possibility that an IT Relation account can be used for lateral movement by a hacker and that an employee can remember a password when no longer employed in IT Relation.

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 are 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.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

We have conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", and additional requirements applicable in Denmark.

Our testing of the design, implementation and functionality of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

Our operating effectiveness testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2 Test actions

The test actions performed when determining the operating effectiveness of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. Furthermore, it is assessed whether controls are being monitored and checked sufficiently and at appropriate intervals. We have tested the specific system set-up on the technical platforms, databases and network components in order to verify whether controls are implemented and have functioned during the period from 1 January 2020 to 31 December 2020. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed.

4.3 Control objectives, control activity, tests and test results

A.5 Control objective: Information security policies

IT Relation's control activity	Control tests performed by PwC	Results of tests
5.1.1 Policies for information security *A set of policies for information security shall be defined, approved by Management, published and communicated to employees and relevant external parties.* IT Relation has a security policy approved by the board of directors. It is available through the Intranet and is distributed to all new employees. The security policy is maintained by the department of compliance and security which reports directly to the board of directors.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that a Management-approved and up-to-date security policy is in place. By inspection, we have verified that the information security policies are communicated to employees and relevant parties.	No significant exceptions noted.
5.1.2 Review of policies for information security *The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.* The security policies are reviewed once a year or whenever new policies are implemented or updated.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that the policies for information security are reviewed at planned intervals or in connection with significant changes. By inspection, we have verified that the security policy is reviewed at least once a year.	No significant exceptions noted.

A.6 Control objective: Organisation of information security

IT Relation's control activity	Control tests performed by PwC	Results of tests
6.1.1 Information security roles and responsibilities *All information security responsibilities shall be defined and allocated.* The responsibility for the information security is located at the board of directors. However, the daily implementation is performed by the department of compliance and security.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No significant exceptions noted.
6.1.2 Segregation of duties *Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.* IT Relation has defined a policy for segregation of duties. The policy is reviewed once a year to ensure that the current level of segregation is still reflecting the information security policy.	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have investigated that the critical operating functions at IT Relation have been appropriately segregated and that primary and secondary operating data have been segregated.	No significant exceptions noted.
6.1.3 Information security risk treatment IT Relation uses risk assessment to evaluate and treat potential risks. Tasks are prioritised based on their risk assessment so the task with the highest score are solved first.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation uses risk assessment to evaluate and treat potential risks. By inspection, we have verified that tasks are prioritised based on their risk assessment.	No significant exceptions noted.

A.7 Control objective: Human resource security

IT Relation's control activity	Control tests performed by PwC	Results of tests
7.1.1 Screening *Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risk.* Prior to employment, IT Relation authenticates the candidate to ensure that the individual is not an imposter, and the candidate's references are checked if applicable. Prior to employment and once a year, the criminal record is examined to ensure its status.	We have briefly discussed the procedures/control activities performed with Management. We have observed that an HR process is in place to ensure that criminal records are presented before employment starts for both employees and external consultants. From a sample of new hires, we observed that criminal records have been acquired before employment start.	No significant exceptions noted.
7.2.1 Management responsibilities *Management shall require all employees and contractors to apply information security in accordance with established policies and procedures of the organisation.* IT Relation has a policy for educating their employees on the information security. All new employees go through an online course, educating the employee on the information security policy.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we observed that signed contracts are in place for employees and suppliers with a view to ensuring that the information security requirements of the organisation are met.	No significant exceptions noted.
7.2.2 Information security awareness, education and training *All employees of the organisation and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.* All new employees at IT Relation receives a welcome email that, among others, contains an introduction video to the security policy.	We have briefly discussed the procedures/control activities performed with Management. We have observed that IT Relation runs introductory courses for new employees during which information security requirements are explained. We have observed that employees are enrolled in mandatory training programmes at regular intervals for the purpose of ensuring compliance with the security requirements of the organisation.	No significant exceptions noted.
7.2.3 Disciplinary process *There should be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.* IT Relation has a communicated process for disciplinary action against an employee who commits an action against the security policy.	We have briefly discussed the procedures/control activities performed with Management. We have observed that disciplinary process is in place and has been communicated to employees to ensure that all employees are aware of consequences of committing an action against security policy.	No significant exceptions noted.

A.7 Control objective: Human resource security

IT Relation's control activity	Control tests performed by PwC	Results of tests
7.3.1 Termination and change of employment *Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.* When an employee leaves IT Relation, the individual is invited to an exit interview. On the agenda is the responsibilities and duties that still apply after the employments has ended.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that employees' access rights to operating systems, networks, databases, etc. are revoked in connection with the termination of employment.	No significant exceptions noted.

A.8 Control objective: Assets Management

IT Relation's control activity	Control tests performed by PwC	Results of tests
8.1.1 Inventory of assets *Assets associated with information and information processing facilities shall be identified, and an inventory of these assets shall be drawn up and maintained.* IT Relation maintains an CMDB database with all assets, and it contains the lifecycle of the asset. Furthermore, IT Relation maintains a list of all systems stating who is the owner of the system and who is technical responsible.	We have briefly discussed the procedures/control activities performed with Management. We have observed that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.	No significant exceptions noted.
8.3.2 Disposal of media *Media shall be disposed of securely when no longer required, using formal procedures.* IT Relation has implemented guidelines for disposing of a medium when it has reached its end of life. IT Relation uses certified vendors for disposing of media to ensure their destruction.	We have briefly discussed the procedures/control activities performed with Management. We have verified that IT Relation has implemented formalised procedures for the processing and destruction of input and output data material.	No significant exceptions noted.

A.9 Control objective: Access control

IT Relation's control activity	Control tests performed by PwC	Results of tests
9.1.1 Access control policy *An access control policy shall be established, documented and reviewed based on business and information security requirements* IT Relation has implemented general guideline for access to customers systems.	We have briefly discussed the procedures/control activities performed with Management. We have observed that guidelines on access controls have been established, reviewed and approved.	No significant exceptions noted.
9.1.2 Access to networks and network services *Users shall only be provided with access to the network and network services that they have been specifically authorised to use.* All access to operating systems, networks, databases and data files made available to new and existing users are 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 briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have observed that access to network and network services is granted based on the employees' job function and manager approvals.	No significant exceptions noted.
9.2.1 User registration and de-registration *A formal user registration and de-registration process shall be implemented to enable assignment of access rights.* IT Relation has a process for registration of users. The process ensures that each user has the access required for their job function and nothing more. When an employee leaves or changes job function, his/her access is either reworked or changed to reflect the new function.	We have briefly discussed the procedures/control activities performed with Management. We have observed that procedures for user administration have been established. By inspection of random samples, we have furthermore observed that the user registration and de-registration process has been implemented.	No significant exceptions noted.
9.2.3 Management of privileged access rights *The allocation and use of privileged access rights shall be restricted and controlled.* IT Relation has a policy for allocation and restriction of users with privileged access. All users with privileged access have a dedicated user with the privileged access. The privileged users access list is audited on a quarterly basis.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation has established formalised procedures for user administration and rights management and that these also apply to users with privileged rights. We have observed that authorisation granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior.	No significant exceptions noted.

A.9 Control objective: Access control

IT Relation's control activity	Control tests performed by PwC	Results of tests
9.2.5 Review of user access rights *Asset owners should review users' access rights at regular intervals.* IT Relation regularly reviews the employees' privileged technical rights in both internal and customer-facing systems. This ensures that rights are in accordance with the employee's work-related need. This review takes place every week. All servers that are user-controlled through ISIM are automatically checked for inactivity for more than 90 days, and inactive accounts are subsequently deleted from the systems in question. Non-technical privileged employees are granted the necessary rights for using internal systems. These default rights are added and removed in connection with employment, transfer and termination at IT Relation.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that user access rights are reassessed once every six months.	No significant exceptions noted.
9.2.6 Removal or adjustment of access rights *The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.* When an employee leaves the company all accesses are reworked. If the employee changes job function, the access is adjusted to reflect the new assignment. Both changes are initiated by the human resource department.	By inspection, we have investigated that regular follow-up is performed on user rights in operating environments and that these rights are granted based on the users' job function. By inspection, we have investigated that terminated users are removed in the operating environment in a timely manner after termination.	No significant exceptions noted.
9.4.1 Information access restriction *Access to information and application system functions shall be restricted in accordance with the access control policy.* IT Relation has a policy of limited access to system and applications to employees who have a work-related need.	By inspection, we have observed that a formal policy for access control that defines allowed technical solutions for authentication is maintained. By inspection of samples of access provision requests, we observed that the user registration and de-registration process has been implemented.	No significant exceptions noted.

A.9 Control objective: Access control

IT Relation's control activity	Control tests performed by PwC	Results of tests
9.4.2 Secure log-on procedures *Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.* IT Relation has a secure logon procedure for access to customer data and systems. No one can access customer data or systems without the use of two factor access.	We have observed that a formal access control policy that defines allowed technical solutions for authentication is maintained. We have observed that the access control policy has been reviewed and approved. We have observed that applications and systems in scope enforce secure log-on procedures.	No significant exceptions noted.
9.4.3 Password management system *Password management systems shall be interactive and shall ensure quality passwords.* IT Relation has a password management system that ensures that the passwords generated are random and uphold the company policy in complexity and length.	By inspection, we have observed that policies have been reviewed and approved. We have observed that policies include: • Application requirements regarding use of passwords • Quality requirements regarding passwords • Requirements regarding lockout policy • Log of and follow-up on failed login attempts • Control of failed login attempts • Requirements regarding use of MFA.	No significant exceptions noted.

A.11 Control objective: Physical and environmental security

IT Relation's control activity	Control tests performed by PwC	Results of tests
11.1.1 Physical security perimeter *Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.* IT Relation has classified its information processing facilities, and access to these are based on this classification. The facilities are divided into three groups. Restricted, limited and open. Visitors are only allowed in open areas or limited if they are escorted by an IT Relation employee. Access to restricted areas are allowed by visitors if they have a work-related need.	By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved.	No significant exceptions noted.
11.1.2 Physical entry controls *Secure areas shall be protected by appropriate entry controls to ensure that only authorised personnel is allowed access.* IT Relation has ensured that access to its restricted areas is secure, that the access to these areas is limited to persons with a work-related need, and that this access is audited frequently.	By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. We have observed that IT Relation has implemented appropriate entry controls to protect physical facilities.	No significant exceptions noted.
11.1.3 Securing offices, rooms and facilities *Physical security for offices, rooms and facilities shall be designed and applied.* IT Relation has implemented limited access to offices. All doors are locked and must be opened by an IT Relation employee. All employees must wear a visible ID with name and picture. All visitors in our customer centres must wear an ID identifying them as visitors. Visitor centres have signs showing visitors where they can roam freely where they are allowed access with an IT Relation employee or where they are not allowed access at all.	By inspection, we observed that a formal physical access and security policy is maintained, reviewed and approved. We have observed that IT Relation has implemented appropriated entry controls to protect physical facilities.	No significant exceptions noted.
11.1.5 Working in secure areas *Procedures for working in secure areas should be designed and applied.* IT Relation has a policy that requires all employees to go through the IT Security manual once a year. Furthermore, employees with access to data centres, data centre infrastructure and data centre network receive additional training before access is granted.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that all guests visiting IT Relation are provided with a visitor's pass and are escorted by an IT Relation employee during the entire visit.	No significant exceptions noted.
11.2.1 Equipment siting and protection	We have briefly discussed the procedures/control activities	No significant exceptions noted.

A.11 Control objective: Physical and environmental security

IT Relation's control activity	Control tests performed by PwC	Results of tests
Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorised access. IT Relation has a policy to ensure the protection of critical equipment.	performed with Management. By inspection, we have observed that IT Relation has established guidelines on the protection against fire, water and heat. We have furthermore observed that IT Relation has obtained an audit report from its subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	
11.2.2 Supporting utilities *Equipment shall be correctly maintained to ensure its continued availability and integrity.* IT Relation ensures that all equipment own by IT Relation is maintained by the manufacturer's specification. Furthermore, IT Relation ensures that its partners do the same.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation has established a fully redundant infrastructure with individual backup.	No significant exceptions noted.
11.2.5 Removal of assets *Equipment, information or software shall not be taken off-site without prior authorisation.* IT Relation has a policy ensuring no employee can remove equipment, information or software without the authorisation of nearest manager or the system owner.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation has established guidelines ensuring that off-site removal of equipment, information or software is subject to authorisation being granted prior to removal.	No significant exceptions noted.
11.2.7 Secure disposal or re-use of equipment *All items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.* IT Relation will ensure that all storage media are disposed of in a verified, secure manner to ensure data cannot be read after removal.	By inspection, we have observed that IT Relation has implemented procedures on secure disposal or re-use of equipment. We have observed that IT Relation has implemented relevant controls in relation to handling the operation of the operating environment.	No significant exceptions noted.

A.12 Control objective: Operations security

IT Relation's control activity	Control tests performed by PwC	Results of tests
12.1.1 Documented operating procedures *Operating procedures shall be documented and made available to all users who need them.* IT Relation has a numbered operations procedure, and it is made available on the intranet. IT Relation separates its operations procedure from its working procedure. The operations procedure is how we do a task (procedural), and the working procedure is what we do with a task (technical).	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that operating procedures have been established and that these are subject to updating at least once a year. We have furthermore observed that the operating procedures are accessible to all relevant employees.	During the audit of operating procedures in the customer environment and during our sample testing, we have observed that the CMDB does not reflect the actual setup of the customers with old contract template and does not contain clear traceability related to special contractual conditions / agreements, including risk letters. We are aware of this fact that it is possible to find special agreements and risk letters if they exist – but there are no formal procedures to ensure that all critical agreements and risk letters with these old customers are registered properly (e.g. in CMDB). IT Relation has informed that there is a plan for renewing these old contracts and thus proper registration of risk letters and special agreements. No further significant exceptions noted.
12.1.2 Change management *Changes to the organisation, business process, information processing facilities and systems that affect information security shall be controlled.* IT Relation has implemented change control on critical infrastructure and for customers who have change control as a business requirement.	We have briefly discussed the procedures/control activities performed with Management. We have observed that IT Relation has drawn up procedures for annual review and updating of: • Incident management • Problem management • Change management • Release and patch management • User administration.	No significant exceptions noted.

A.12 Control objective: Operations security

IT Relation's control activity	Control tests performed by PwC	Results of tests
12.1.3 Capacity management *The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.* IT Relation has drawn up procedures for monthly reporting on operations. These reports include information on production environment operations, including information on capacity. Automatic monitoring of the operating environment and relevant system parameters has been established, including of capacity, to ensure that future capacity requirements are met.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that reports on production environment operations at IT Relation are sent to customers each month. We have furthermore observed that the capacity of production systems at IT Relation is monitored to ensure that future capacity requirements are met.	During the review of capacity management procedures, we observed that there are quarterly meetings where the total capacity is reviewed. However, during our inspection we did not receive sufficient documentation showing that the procedure has also been implemented / that meetings have been held. No significant exceptions noted.
12.2.1 Controls against malware *Detection, prevention and recovery controls to protect against malware shall be implemented, combined with the appropriate user awareness.* IT Relation has implemented a procedure for ensuring a working antivirus software on all applicable systems. The antivirus software is monitored.	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have observed that the employees' computers at IT Relation are protected by antivirus software – and that this software is up to date.	No significant exceptions noted.
12.3.1 Information backup *Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.* IT Relation performs backup in accordance with IT Relation's best practice or customers' business requirement. The backup jobs are monitored to ensure their continuous operation. Yearly a recovery test initiated by IT Relation is performed.	We have briefly discussed the procedures/control activities performed with Management. We have observed that requirements regarding backup have been established in the contract with sub-contractors that provide services where backup is relevant. We have observed that a full restore test of IT environments has been performed.	No significant exceptions noted.
12.4.1 Event logging *Event logs recording users' activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.* IT Relation has implemented a monitoring system which should ensure that the customers' systems are up and running. The system is monitored 24/7 by the operations department.	We have briefly discussed the procedures/control activities performed with Management. We have observed that event logging of user activities, exceptions, faults and information security events has been configured. We have observed that a log documentation overview stipulates when log reviews must be performed.	No significant exceptions noted.

A.12 Control objective: Operations security

IT Relation's control activity	Control tests performed by PwC	Results of tests
12.4.2 Protection of log information *Logging facilities and log information shall be protected against tampering and unauthorised access.* IT Relation records logs for different systems at different security levels. For ordinary performance and uptime data, there are no separation of duty. For the SIEM system, the separation of duty is full. The only employees who have access to delete log data have no access to customer and IT Relation systems.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation has established logging facilities that are accessible only to employees whose job function justifies such access. We have observed that log information cannot be edited or deleted. Also, IT Relation performs backup of the log information several times a day, and access is restricted to a few people.	No significant exceptions noted.
12.4.3 Administrator and operator logs *System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.* All access to customer systems is logged in the assets management system. The access log is stored securely, and the system is set up to audit who, if any, tries to alter the information stored. The Compliance & Security department is notified if someone alters the data.	We have briefly discussed the procedures/control activities performed with Management. Furthermore, we have verified that logging parameters are set up to ensure that actions performed by users with extended access rights are logged. By random inspection, we have also verified that adequate follow-up on logs from critical systems is performed.	No significant exceptions noted.
12.4.4 Clock synchronisation *The clocks of all relevant information-processing systems within an organisation or security domain should be synchronised to a single reference time source.* IT Relation has synchronised all relevant information-processing systems to a single reference time source.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation has established a reference time source for clock synchronisation of all relevant information-processing systems.	No significant exceptions noted.
12.5.1 Installation of software on operational systems *Procedures shall be implemented to control the installation of software on operational systems.* IT Relation has defined a set of standard implementation description. These systems are allowed on customer systems.	We have briefly discussed the procedures/control activities performed with Management. Using random samples from the system used for documenting changes, we have investigated whether – in accordance with guidelines – changes to the operating environment are carried out utilising a controlled process, including whether: • an approved test is performed prior to changes being implemented • testing and approval of emergency changes to the operating environment are documented immediately after being implemented.	No significant exceptions noted.

A.12 Control objective: Operations security

IT Relation's control activity	Control tests performed by PwC	Results of tests
12.7.1 Information systems audit controls *Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.* IT Relation uses standard best practices to ensure that enough variables are being monitored, without the monitoring impacting the system performance negatively. This is done in large part by using third-party systems developed to the task.	We have briefly discussed the procedures/control activities performed with Management. Furthermore, we have verified that logging parameters are set up to ensure that actions performed by users with extended access rights are logged. By random inspection, we have also verified that adequate follow-up on logs from critical systems is performed.	No significant exceptions noted.

A.13 Control objective: Communication security

IT Relation's control activity	Control tests performed by PwC	Results of tests
13.1.1 Network security management *Networks shall be managed and controlled to protect information in systems and applications.* IT Relation has implemented several policies to ensure a secure communication and that tampering of data is minimised. Access to network devices is limited to employees with a work-related need. Communication between IT Relation and customer sites is performed by valid and proven secure technologies.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have investigated whether – in accordance with guidelines – an appropriate security architecture has been established in the network, including whether: • the network is segregated into secure zones and whether customer environments are separated from IT Relation's own environment • remote access is granted through two-factor authentication • changes to the network environment included in our sample have been made in a controlled manner in accordance with the change management rules.	No significant exceptions noted.
A.13.1.3 Segregation in networks *Groups of information services, users and information systems shall be segregated on networks.* IT Relation segregates customer network in one or more networks, depending on the need for segregation. Customers are not able to access other customer networks.	We have briefly discussed the procedures/control activities performed with Management. We have reviewed the technical security architecture and, by inspection of random samples, we have investigated whether – in accordance with guidelines – an appropriate security level has been established, including whether: • secure zones and customer environments are separated from IT Relation's own environment • access to the network is segregated into relevant user groups based on users' work-related need.	No significant exceptions noted.
A.13.2.1 Information transfer policies and procedures *Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.* IT Relation has a network policy that describes who is responsible for ensuring secure and reliable communication channels.	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have investigated whether a sufficient network policy has been implemented to ensure secure network communication.	No significant exceptions noted.

A.14Control objectives: System acquisition, development and maintenance

IT Relation's control activity	Control tests performed by PwC	Results of tests
14.1.1 Information security requirements analysis and specification *The information security-related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.* IT Relation performs a risk assessment of all new systems they acquire. This is done to ensure that the system meets IT Relation policies regarding information security.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that IT Relation has established a security organisation enforcing an appropriate level of information security in systems.	No significant exceptions noted.

A.15 Control objective: Supplier relationships

IT Relation's control activity	Control tests performed by PwC	Results of tests
15.1.1 Information security policy for supplier relationships *Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets shall be agreed with the supplier and documented.* IT Relation performs a yearly risk assessment of its suppliers. This is done to ensure they still live up to the security requirements that IT Relation expects.	We have observed that a formal and documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From a sample of signed contracts, we observed that information security requirements have been contractually agreed. From a sample of months, we observed that IT Relation audits key suppliers on a periodic basis, based on agreed information security requirements. We have observed that third-party declarations have been received and processed by IT Relation for key suppliers.	No significant exceptions noted.
15.2.1 Monitoring and review of supplier services *Organisations shall regularly monitor, review and audit supplier service delivery.* IT relation performs a yearly risk assessment of all suppliers. In addition, the most critical suppliers like hardware, data centre and software suppliers for the data centre undergo a more comprehensive risk assessment.	We have observed that a formal, documented procedure is in place to ensure that new or re-negotiated application or service supplier contracts are validated against a list of defined information security requirements. From a sample of signed contracts, we observed that information security requirements have been contractually agreed. From a sample of months, we observed that IT Relation audits key suppliers on a periodic basis, based on agreed information security requirements. We have observed that third-party declarations have been received and processed by IT Relation for key suppliers.	No significant exceptions noted.

A.16 Control objective: Information security incident management

IT Relation's control activity	Control tests performed by PwC	Results of tests
16.1.1 Responsibilities and procedures *Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.* IT Relation has a procedure outlining the management and reporting during an information security breach. Every employee in IT Relation has been informed what to do in an event or discovery of a security issue to ensure a quick response and to ensure lessons are learned.	We have observed that a formal and documented incident management process has been reviewed and approved. We have observed that a formal and documented incident management process has been implemented. We have observed that the incident management process has been communicated to employees. We have observed that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system.	No significant exceptions noted.
16.1.2 Reporting and handling information security events and security breach *Information security events should be reported through appropriate management channels as quickly as possible.* Employees and contractors using the organisation's information systems and services should be required to note and report any observed or suspected information security weaknesses in systems or services. Information security events are reported through appropriate management channels as quickly as possible.	We have observed that a formal and documented incident management process has been implemented. We have observed that the incident management process has been communicated to employees. We have observed that all incidents have been registered, that necessary actions have been performed, and that the solutions have been documented in an incident management system and reported through the Information Security Board.	No significant exceptions noted.

A.17 Control objective: Information security aspects of business continuity management

IT Relation's control activity	Control tests performed by PwC	Results of tests
17.1.1 Planning information security continuity *The organisation shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.* IT Relation has a disaster recovery plan for how IT Relation can get back into production as quickly as possible during a disaster. The disaster recovery plan is tested once a year.	We have observed that a formal and documented business continuity plan is maintained, reviewed and approved annually. We have observed that a business impact assessment has been performed to establish the requirements of a business continuity plan. We have observed that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No significant exceptions noted.
17.1.2 Implementing information security continuity *The organisation shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.* IT Relation has implemented a contingency plan for each of its critical systems so that customers experience as little inconvenience as possible during the loss of a critical system.	We have observed that a formal and documented business continuity plan is maintained, reviewed and approved annually. We have observed that a business impact assessment has been performed to establish the requirements of the business continuity plan.	No significant exceptions noted.
17.1.3 Verifying, reviewing and evaluating information security continuity *The organisation should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.* The organisation verifies the established and implemented information security continuity controls at regular intervals to ensure that they are valid and effective during adverse situations.	We have observed that underlying procedures for the business continuity are reviewed and updated. We have observed that the underlying procedures have been tested to ensure that they are valid and effective during adverse situations.	No significant exceptions noted.

A.18 Control objective: Compliance

IT Relation's control activity	Control tests performed by PwC	Results of tests
18.1.1 Identification of applicable legislation and contractual requirements *All relevant legislative statutory, contractual requirements and the organisation's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system.* IT Relation uses standard contracts. If a customer cannot meet its business requirement within the standard contract, a personalised contract can be agreed upon. In such a situation, the contract is eventually owned by a service delivery manager who will be responsible for implementing clauses not part of a standard contact.	We have observed that a formal policy for complying with relevant legislation is maintained, reviewed and approved.	No significant exceptions noted.