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 2023 to 31 December 2023 in relation to IT Relation's hosting services

January 2024

pwc

Contents

1 Management's statement

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

IT Relation A/S uses Fuzion and InterXion as subservice suppliers for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that Fuzion and InterXion perform for IT Relation A/S.

IT Relation A/S uses B4Restore and Keepit as subservice suppliers for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore and Keepit perform for IT Relation A/S.

Some of the control objectives stated in our description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

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 2023 to 31 December 2023. The criteria used in making this statement were that the accompanying description:

   (iii) Presents how IT general controls in relation to the 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 the hosting services during the period from 1 January 2023 to 31 December 2023

   (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 the 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 2023 to 31 December 2023. 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 2023 to 31 December 2023.

Herning, 31 January 2024
IT Relation A/S

Frank Bech Jensen
Head of Compliance and Security

IT Relation A/S
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 2023 to 31 December 2023 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 its hosting services which have processed customers' transactions throughout the period from 1 January 2023 to 31 December 2023 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

IT Relation uses Fuzion and InterXion as subservice suppliers for housing services. This report uses the carve-out method and does not comprise control objectives and related controls that Fuzion and InterXion perform for IT Relation.

IT Relation uses B4Restore and Keepit as subservice suppliers for backup services. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore and Keepit perform for IT Relation.

Some of the control objectives stated in IT Relation's description in section 3 can only be achieved if the complementary controls at the customers are suitably designed and operating effectively with IT Relation's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

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 in the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional conduct, as well as ethical requirements applicable in Denmark.

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or 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 the 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 the hosting services were designed and implemented throughout the period from 1 January 2023 to 31 December 2023;

b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 January 2023 to 31 December 2023; 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 2023 to 31 December 2023.

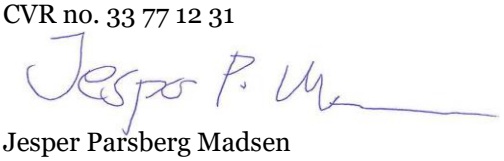
Description of test of controls

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, 31 January 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31



Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Iraj Bastar
Director

3 IT Relation's description of IT general controls at IT Relation A/S relating to financial reporting for its hosting services

From 1 January 2023 to 31 December 2023 the company has provided services in accordance with the information security management systems documented in the system description of the ISAE 3402 assurance report for 2023 and in compliance with ISO 27001:2022.

Organisational changes at IT Relation, Me'ning and itm8

On 15 November 2023, itm8 announced the initiation of a comprehensive corporate merger involving all of their companies. Specifically, this means that, from this date, itm8 will begin the process of merging their 13 companies into a single entity under the name itm8.

The merger process is expected to be completed over the course of 2024. Despite this announcement being made on 15 November 2023, it is not expected to impact deliveries that have been audited in the period from 1 January 2023 to 31 December 2023 which are covered by this assurance report.

The consolidated itm8 entity will ultimately deliver all its services through four key service areas:

- Cloud & Infrastructure
- IT Security
- Digital Transformation
- Application Services.

By consolidating all activities under one itm8 umbrella, we aim to create an extraordinary and attractive workplace for the most competent IT specialists. This initiative aims to strengthen our deliveries and service, which our clients will experience positively.

As the revised delivery does not change within the audit period, the companies IT Relation A/S, Me'ning, and itm8 will continue to be named in the report as usual.

Further information about itm8's corporate merger can be found by following this link: itm8 unites 13 companies in a major merger

3.1 Introduction to IT Relation A/S

IT Relation A/S is a leading IT company dedicated to optimising client business through IT solutions. Our expertise encompasses IT strategy, hosting, service desk, support and hardware. With a staff of 700 people, spread across Denmark with offices in Herning, Aarhus, Copenhagen, Kolding and Aalborg, and an international presence in the Czech Republic and the Philippines, we work purposefully to meet our customers' needs.

IT Relation A/S operates within four key business areas:

- Managed Services (IT outsourcing and hosting)
- Service Desk
- IT Security
- Hardware.

Our goal is to function as a complete end-to-end provider of IT solutions by implementing a 360-degree approach. Our competent and smiling IT problem solvers are available around the clock, 365 days a year, at our service desks.

We strive to deliver optimal IT solutions and unparalleled customer service every single day.

3.2 Introduction to itm8

IT Relation A/S is an integral part of itm8, a significant IT conglomerate consisting of 13 companies and over 1700 employees. Itm8's core mission is to consolidate expertise in IT under one umbrella, enabling the delivery of comprehensive end-to-end solutions to our customers. Within this structure, IT Relation A/S contributes significantly to the conglomerate's overall portfolio.

The itm8 group, with over 100 dedicated employees, is focused on enhancing operational efficiency and creating synergies among its subsidiaries. This is achieved through a range of internal service functions, including:

- Data Center
- Internal Development
- Internal IT
- Human Resources
- Marketing
- Finance
- Legal
- Compliance & Security.

In connection with the ISAE 3402 accounting reporting, itm8's group functions are included as IT Relation A/S utilises these internal services to their full extent, and itm8's service functions are also covered by IT Relation's information security management system. This integrated approach ensures a cohesive and efficient support structure, crucial for the services and success of IT Relation A/S.

3.3 Introduction to Me'ning

IT Relation A/S is the parent company of Me'ning, a dynamic enterprise specialised in developing Microsoft-based and customised solutions. Me'ning engages in the entire spectrum of the IT development process, from initial needs assessment to detailed follow-up, thus ensuring the delivery of solutions that are both high-quality and precisely tailored to the client's unique requirements.

Me'ning's expertise spans both digital transformation and specialised development, enabling them to create effective and user-specific systems. Their range of Microsoft solutions includes, but is not limited to:

- Modern Workplace
- CRM Solutions
- Data and Analytics
- Baseline Tools (including reporting, GDPR, Workplace, Whistleblower)
- SharePoint Development
- Custom Development.

In addition to these, Me'ning also develops and maintains a range of proprietary systems such as Secure Mail, Patient Journal solutions, OnlineLegat and VirkCollect.

With a talented staff of 70 employees spread across three offices in Copenhagen, Aarhus and Herning, Me'ning holds a strong position in the market. In connection with the ISAE 3402 accounting reporting, Me'ning is also included, as it, being a subsidiary of IT Relation A/S, fully utilises the same management system as both the itm8 group function and IT Relation A/S. This ensures a consistent and high standard in all operational and administrative aspects.

3.4 Introduction to the description of services

This description has been crafted with the aim of furnishing information for use by IT Relation's customers and their auditors in compliance with the Danish Standard on Assurance Engagements concerning controls within a service organisation: ISAE 3402. The description encompasses details about the system and control environment established within IT Relation's operational and hosting services provided to their customers.

This document includes explanations of the procedures implemented to ensure the satisfactory operation of systems. The objective is to present adequate information to enable the auditors of hosting customers to independently evaluate the identification of risks related to control weaknesses in the control environment, particularly those that may pose a risk of material misstatement in customers' IT operations for the period from 1 January 2023 to 31 December 2023.

3.5 Description of IT Relation's services

Since its establishment in 2003, IT Relation has been a prominent player in the hosting industry where we have delivered advanced IT solutions to a wide range of industries. Our expertise extends far beyond hosting as we offer a diversified spectrum of IT-related services.

Our services for the hosting market include:

- Hosting and housing
- Remote Backup
- Operations and operational management
- Cloud-based solutions
- Service desk.

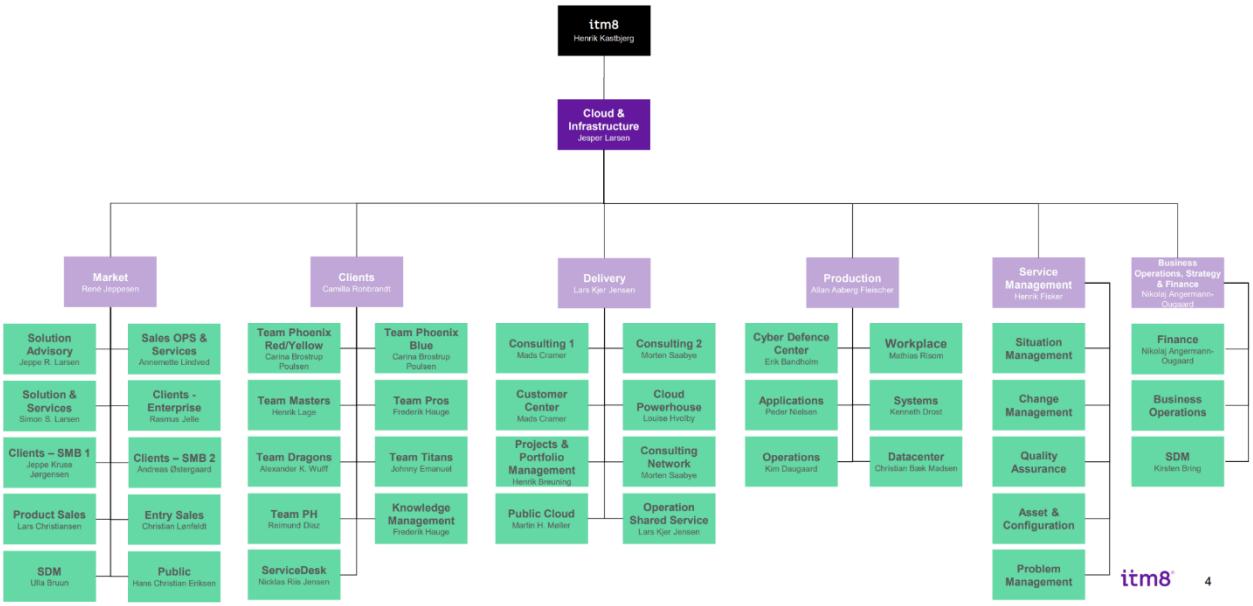
Our system description provides a detailed overview of the working processes used and the controls implemented in relation to these services.

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

- Development of IT solutions
- Consulting and services in IT security at both management and technical levels
- Strategic consulting at the CIO level
- Technical project management
- Technical support and on-site service.

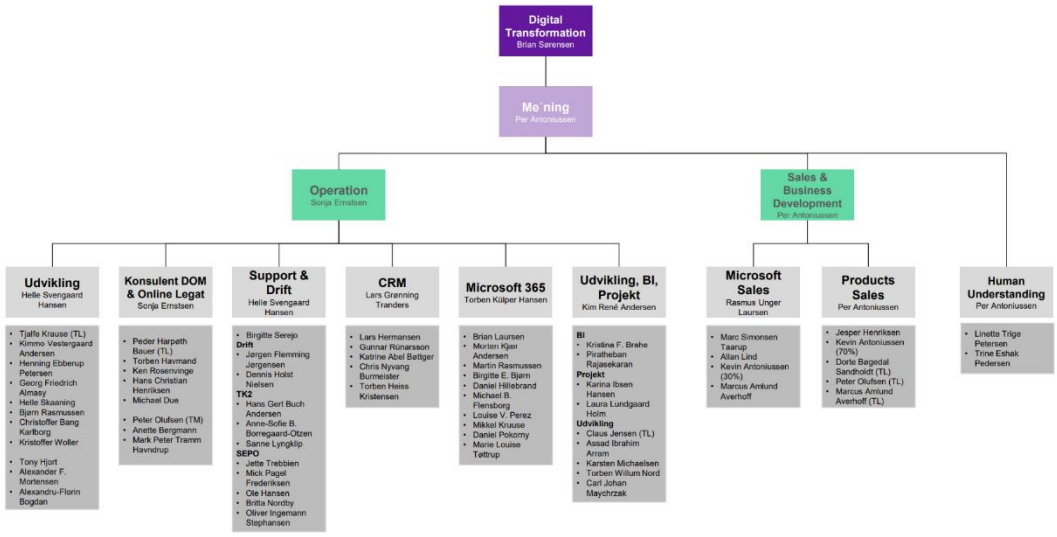
Our goal is to provide comprehensive and quality-oriented IT solutions that meet our clients' unique needs and effectively support their business.

3.6 IT Relation's organisation



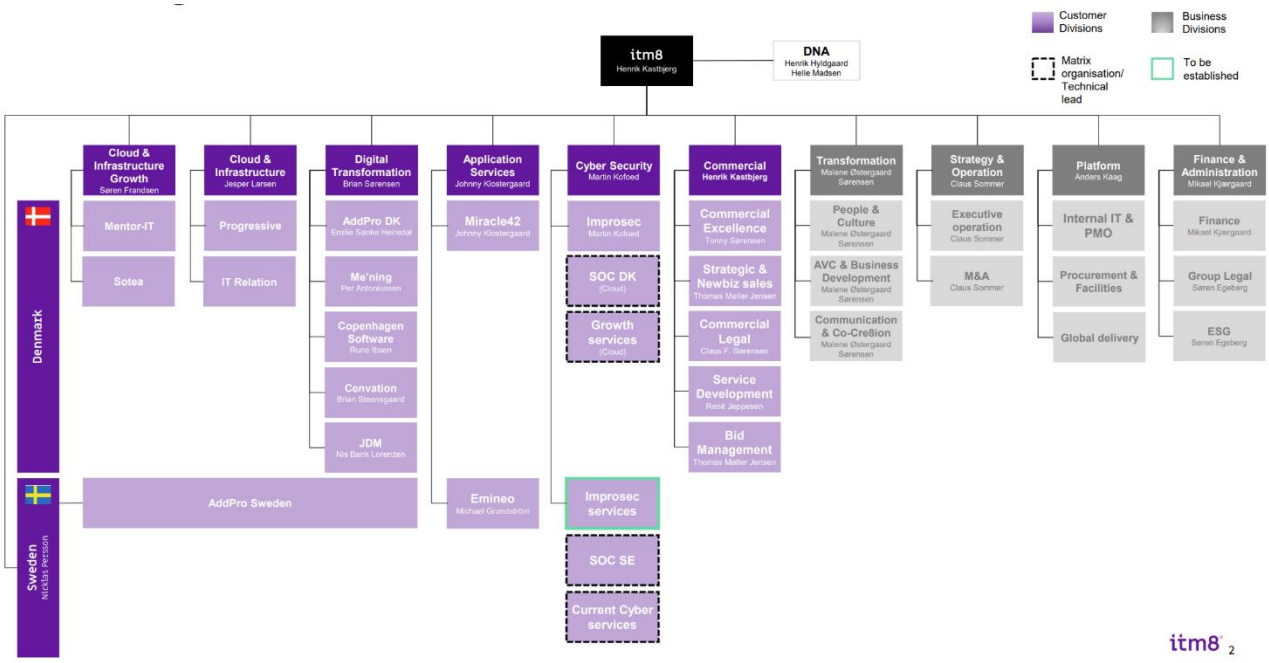
Organisational chart – IT Relation A/S

3.7 Me'ning's organisation



Organisational chart – Me'ning

3.8 Itm8's organisation



Organisational chart – itm8

3.9 Risk management at IT Relation

Risk management at IT Relation is a multi-dimensional and systematic process that occurs across various areas and levels within the organisation. Annually, a thorough risk and threat assessment of the company's internal systems is conducted. This assessment is a collective effort where input is gathered from throughout the company. The security department facilitates this process and prepares a first draft which is presented to IT Relation's Management. After an internal review and discussion, these assessments are officially approved by Management.

In connection with projects, detailed security assessments and analyses of potential special risks and uncertainties are carried out based on the nature of the project. These assessments are conducted following an established and structured procedure.

At the operational level of project management, continuous risk management is implemented. This management follows a defined project management model, where the primary responsibility for project-related risk management lies with the project manager. In this process, it is common for the project manager to involve project participants, external partners and possibly a steering group to ensure a comprehensive and effective risk management approach.

3.10 Control framework, control structure and criteria for control implementation

IT Relation has established an information security policy and comprehensive control processes that cover all systems and services provided to customers. These security measures are constantly being improved and adapted, which is managed in collaboration with highly qualified specialists.

As an ISO/IEC 27001:2022-certified company, IT Relation implements and complies with the requirements of the standard. This includes the establishment of an information security management system (ISMS), which enables:

- Monitoring and assessing the status of information security
- Performing internal audits
- Conducting internal audits to evaluate security measures and their effectiveness
- Implementing management reviews with top management.

The purpose of the ISMS is to ensure continuous monitoring and adjustment of the information security level in relation to the general threat landscape. The system is the foundation for a continuous improvement process which ensures effective handling of incidents and a continuous increase in the level of information security.

Annually, IT Relation undergoes an IT audit, resulting in an audit report in accordance with the ISAE 3402 standard. The implemented and revised control measures are consistent with Annex A of the ISO/IEC 27001:2022 standard.

The control areas and activities from this control framework are implemented in accordance with best practices to minimise risks associated with IT Relation's services. The following control areas from the chosen model are integrated into the overall control environment:

- Information security policies
- Organisation of information security
- Human resource security
- Access control
- Physical and environmental security
- Protection against environmental factors
- 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.

Detailed descriptions of each of these 15 areas are found below.

Information security policies	
Objective	Based on an IT risk analysis, a management-approved information security policy, along with supporting topic-specific policies, has been developed and communicated to relevant employees in the company.
Procedures and controls	IT Relation identifies relevant IT risks to which the established services are exposed. This is managed through a current threat and risk assessment in IT Relation, both in connection with all development projects and changes in system environments and through an annual reassessment of the risk assessment. The result of the annual review is presented to Management. IT Relation also provides information to hosting customers' auditors for their assessment of IT Relation as a service provider. In addition to operational matters, IT Relation can also provide information about security issues if required by customers.
Time of performing the control	The information security policy and topic-specific policies are reassessed at least once a year, before the IT audit is conducted, and a statement is issued.
Who performs the control	The annual review is performed by Compliance & Security.

Control documentation	The information security policy as well as topic-specific policies are subject to document control.

Organisation of information security

Objective	To manage information security within the organisation.
Procedures and controls	The primary responsibility for information security lies with the executive management of IT Relation. This ensures that procedures and systems always support compliance with the applicable IT security policy. Compliance & Security describes the overarching objectives, and the operations manager is responsible for the development and implementation of relevant controls to comply with the information security policy and topic-specific policies. The security level must be measurable and controllable where possible, and it should reflect best practices within the individual control activities in the areas where services are offered to customers. Information security initiatives are continuously discussed at Continuous Improvement meetings held by Compliance & Security, after which new and improved initiatives are communicated and aligned with the operations manager and Management. The following employees are responsible for anchoring the outcomes of Continuous Improvement meetings: • CTO: Anders Kaag • Head of Compliance & Security: Frank Bech Jensen • Information Security Manager: Nils Lau Frederiksen • Information Security Officer: Jeppe Gottlieb • Compliance Manager: Bo Duholm Hansen • Security Director: Johnni Meldgård Rude • Head of Cyber Defense Center: Erik M. L. Bandholm • Director of Internal IT: Thomas Møller • Technical Cloud Architect: Flemming Laursen • Cloud Citrix Specialist: Jakob Thalund Jensen • Data Center Network Team Manager: Dan Sørup Olesen • Data Center Specialist: Jakob Andersen
Time of performing the control	Continuous Improvement meetings are held bi-monthly.
Who performs the control	Continuous Improvement meetings are held by Compliance & Security who communicates to the information security responsible.
Control documentation	Continuous Improvement meetings are documented in meeting minutes, and derived initiatives are further documented in activity logs.

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 IT security, and the terms include the current IT security policy and guidelines in addition to describing

	the secrecy and confidentiality agreement. Criminal records are checked each year. Management must ensure that all employees implement and maintain IT security in accordance with the IT and Information Security Policy for IT Relation A/S. 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 and Information Security Policy for IT Relation A/S. • That they are motivated to live up to the IT and Information Security Policy for IT Relation A/S and achieve a level of attention in questions related to IT security that is consistent with their role and responsibilities in IT Relation. • That they adhere to the guidelines and regulations for the recruitment, including the IT and Information Security Policy for IT Relation A/S. • 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 and Information Security Policy for IT Relation A/S.
Retirement or termination	Responsibilities and obligations relating to information security which remain valid after termination or amendment of employment conditions are defined and communicated to the employee or the consultant – and enforced. When an employee resigns from IT Relation, the employee's direct manager is responsible for ensuring that all equipment is returned and that the retired access rights to information systems cease. Tasks and responsibilities in connection with termination of employment are described in the Retirement Policy. The purpose is to ensure that the resigned employee is aware of and understands his/her responsibility after termination from IT Relation. At the end of the employment, it must be ensured that the resigned employee is informed of applicable IT security requirements and legal rules. The confidentiality agreement continues after the resignation, and the resigned employee is expressly informed before the resignation.
Time of performing the control	At the time of employment and during our internal 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 Relation's 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 operations department of 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 operations department of IT Relation is responsible for ensuring that the procedure for third-party access to the customer's environment is observed as agreed 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 a service request in the service request management system, detailing the scope of the third-party access.

Physical and environmental security

IT Relation has primary and secondary data centres where IT equipment is placed. Every data centre has a data centre manager.

Physical access control and security	
Objective	The physical access to systems, data and other IT resources is limited to and planned with the data centre manager.
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 operations department and the housing provider perform the controls. Controls of the handing out of 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, water 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 power supply 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	The check is carried out by service providers.
Who performs the control	All control forms are located at the housing suppliers.
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 backup copy of data is made and stored in order to restore the data if lost. IT Relation makes an assessment and a follow-up of any errors in the backup.
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 and Information Security Policy for IT Relation A/S. The operating procedures are prepared by the Operations department in close cooperation with the customer and third-party providers. Operations are handled through the platform tools of the Citrix servers. Several job descriptions for the Operations department define which surveillance and checks are performed daily, weekly and annually. Errors found in the controls performed and any errors from the systematic surveillance systems are corrected as soon as possible by means of procedures or best practice. The customer is immediately informed about the extent and the implications of the errors observed. The following functional areas have access to the customers' IT systems: • Service desk employees • Operations employees • Consultants.
Time of performing the control	The control is performed 24/7 or in the primary operating time according to the SLA agreement with the individual customer.
Who performs the control	Controls are performed by the Operations department at IT Relation. The operations centre is monitored 24/7 at one or more of our locations in Herning and Viby, and, if the customers have agreed to it, IT Relation's 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 on 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 Relation • 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 Relation's 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 IT Relation's 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 is 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 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 is provided within the agreed timeframe.
Procedures and controls	IT Relation has established a set of written service desk procedures in the areas agreed 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 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 at 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.

3.11 Contingency plans

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

Vital systems that will be restarted within 24 hours include:

- 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.

3.12 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.

3.13 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.

3.14 Complementary controls at customers

Matters to be considered by the customers' auditors

Services provided

The above system description of controls is based on IT Relation's standard terms. Consequently, the customers' deviations from IT Relation's standard terms are not comprised by this report.

The customers' own auditors should therefore assess whether this report can be extended to the specific customer and identify any other risks, which are 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 IT Relation's customers.

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

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 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 **Error! Reference source not found.**. Any other control objectives, related controls and controls at customers are not c overed 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 2023 to 31 December 2023. 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

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.1	**Policies for information security** *Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.* IT Relation has defined and documented an Information Security Policy which is approved by top management and distributed to all employees. IT Relation has defined and documented several topic-specific policies which support the Information Security Policy and is distributed to all relevant employees. The Information Security Policy and topic-specific policies are reviewed at least annually or if significant changes occur.	We inquired Management regarding the procedures/control activities performed. We inspected that a Management-approved and updated security policy is in place. We inspected that the information security policies are communicated to employees and relevant parties and is reviewed annually.	No exceptions noted.
5.2	**Information security roles and responsibilities** *Information security roles and responsibilities shall be defined and allocated according to the organisation's needs.* IT Relation has established and defined roles and responsibilities with a correlation to the information security management system.	We inquired Management regarding the procedures/control activities performed. We inspected that the organisational areas of responsibility have been defined and allocated to relevant personnel.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.3	**Segregation of duties** *Conflicting duties and conflicting areas of responsibility shall be segregated.* IT Relation has defined policies for segregation of duties which are reviewed at least annually or if significant changes occur to ensure the level of segregation reflect the Information Security Policy and the appropriate level of segregation needed.	We inquired Management regarding the procedures/control activities performed. By inspection of random samples, we investigated that the critical operating functions at IT Relation have been appropriately segregated and that primary and secondary operating data have been segregated.	No exceptions noted.
5.4	**Management responsibilities** *Management shall require all personnel to apply information security in accordance with the established information security policy, topic-specific policies and procedures of the organisation.* IT Relation requires Management to familiarise themselves and support applicable information security initiatives and educate their employees on these initiatives.	We inquired Management regarding the procedures/control activities performed. We inspected that Management is familiar with information security initiatives.	No exceptions noted.
5.5	**Contact with authorities** *The organisation shall establish and maintain contact with relevant authorities.* IT Relation has established and implemented communication procedures for how to communicate with relevant authorities in case of a security incident.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation has a communications procedure for how to communicate with relevant authorities in the case of a security incident.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.7	**Threat intelligence** *Information relating to information security threats shall be collected and analysed to produce threat intelligence.* IT Relation produces threat intelligence from various sources including vulnerability reports, selected news sources, suppliers, authorities and special interest groups to be used for risk-based decision making.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation collects and analyses information of information security threats.	No exceptions noted.
5.9	**Inventory of information and other associated assets** *An inventory of information and other associated assets, including owners, shall be developed and maintained.* IT Relation has implemented and maintains various CMDB's depending on the nature of the assets in scope. This includes databases on endpoints, servers, networking equipment, databases etc. all of which have owners and other relevant information allocated to them.	We inquired Management regarding the procedures/control activities performed. We inspected that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.	No exceptions noted.
5.10	**Acceptable use of information and other associated assets** *Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.* IT Relation has established and implemented rules on acceptable use of IT Relation's assets documented in our Policy for Acceptable Use.	We inquired Management regarding the procedures/control activities performed. We inspected that adequate controls are in place to ensure rules on acceptable use and procedures for handling information in IT Relation.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.12	**Classification of information** *Information shall be classified according to the information security needs of the organisation based on confidentiality, integrity, availability, and relevant interested party requirements.* IT Relation has established a Data Classification Scheme addressing how various type of data must be classified and handled according to their classification.	We inquired Management regarding the procedures/control activities performed. By inspection, we verified that information is classified and that a Data Classification Scheme has been implemented.	No exceptions noted.
5.14	**Information transfer** *Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organisation and between the organisation and other parties.* IT Relation has established policies and procedures for information transfer to ensure that information travels through secure and reliable communication channels.	We inquired Management regarding the procedures/control activities performed. We inspected that an appropriate security architecture has been established in the network and that information transfer rules are in place.	No exceptions noted.
5.15	**Access control** *Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.* IT Relation has implemented general guidelines for access to its own and customer system's based on business and information security requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that guidelines on access controls have been established, reviewed and approved.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.18	**Access rights** *Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organisation's topic-specific policy and rules for access control.* IT Relation regularly reviews the employee's privileged technical rights in both internal and customer-facing systems to ensure rights are appropriate and in accordance with the employee's work-related need. 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. When an employee leaves IT Relation, all accesses are revoked. If an employee changes job function, the access is adjusted to reflect the new assignment.	We inquired Management regarding the procedures/control activities performed. By inspection, we investigated that terminated users are removed in the operating environment in a timely manner after termination. Furthermore, we inspected that user access rights are reassessed once every six months.	No exceptions noted.
5.19	**Information security in supplier relationships** *Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of a supplier's products or services.* IT Relation has established procedures for managing security risks associated with the use of a supplier's products and services which include a yearly risk assessment and audit of suppliers to ensure suppliers continue to live up to the security requirements that IT Relation expects.	We inspected 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 samples of signed contracts, we inspected that risk assessments are performed regularly on critical suppliers. Furthermore, we inspected that IT Relation audits key suppliers on a periodic basis, based on agreed information security requirements.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.20	**Addressing information security within supplier agreements** *Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.* IT Relation has established security requirements for suppliers, which is being addressed as part of the contractual agreement with the suppliers and the general Terms and Conditions for Suppliers collaborating with IT Relation.	We inspected 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.	No exceptions noted.
5.22	**Monitoring, review, and change management of supplier services** *The organisation shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.* IT Relation has established procedures for managing security risks associated with the use of a supplier's products and services which include a yearly risk assessment and audit of suppliers to ensure supplier continue to live up to the security requirements that IT Relation expects. If changes of supplier services affect customer environments, services or infrastructure, these changes are subject to be managed in IT Relation's change management process as well.	We inspected 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 inspected that information security requirements have been contractually agreed. From a sample of months, we inspected that IT Relation audits key suppliers on a periodic basis, based on agreed information security requirements. We inspected that third-party declarations have been received and processed by IT Relation for key suppliers.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.23	**Information security for use of cloud services** *Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organisation's information security requirements.* IT Relation has established a strategy for the use of cloud services in accordance with IT Relation's information security requirements, including the use, management and exit from cloud services.	We inspected that a strategy for the use of cloud services has been established.	No exceptions noted.
5.24	**Information security incident management, planning and preparation** *The organisation shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.* IT Relation has defined, established and implemented a plan for managing information security incidents which includes a process for incident management and handling, and the roles and responsibilities related to incident response.	We inspected that a formal and documented incident management process has been implemented. We inspected that roles and responsibilities related to the incident management process has been communicated to employees.	No exceptions noted.
5.26	**Response to information security incidents** *Information security incidents shall be responded to in accordance with the documented procedures.* IT Relation has established procedures for responding to information security incidents.	We inspected that a formal and documented incident management process has been implemented. We inspected 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 exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.27	**Learning from information security incidents** *Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.* IT Relation has established procedures for learning from information security incidents according to which security incidents are continuously reviewed for learning opportunities and improvement of IT Relation's security posture.	We inspected that a formal and documented incident management process has been implemented. We inspected that all incidents have been registered, that necessary actions have been performed, and that security incidents have been reviewed.	No exceptions noted.
5.29	**Information security during disruption** *The organisation shall plan how to maintain information security at an appropriate level during disruption.* IT Relation has established business continuity plans to ensure that IT Relation can maintain information security and operations at an appropriate level during disruption.	We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually. We inspected that underlying procedures related to the business continuity plan have been reviewed and approved by appropriate personnel.	No exceptions noted.
5.30	**ICT readiness for business continuity** *ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.* IT Relation performs ICT readiness tests annually to ensure that business continuity plans can support the intended and appropriate outcome and that the organisation acts according to business continuity plans.	We inspected that a formal and documented business continuity plan is maintained, reviewed and approved annually. We inspected that ICT readiness tests are performed annually and approved by relevant personnel.	No exceptions noted.

Control objective 5:
Organisational controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
5.34	**Privacy and protection of PII** *The organisation shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.* IT Relation has identified applicable requirements regarding the preservation of privacy and protection of PII and established adequate controls and measure to meet these requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation has established requirements regarding the preservation of privacy and protection of PII.	No exceptions noted.
5.37	**Documented operating procedures** *Operating procedures for information processing facilities shall be documented and made available to personnel who need them.* IT Relation has established adequate and documented operating procedures to support and manage the operation of solution and services provided by IT Relation. This includes establishing a platform for communication and availability of these operating procedures to employees with a work-related need for them.	We inquired Management regarding the procedures/control activities performed. We inspected that operating procedures have been established and that these are subject to updating at least once a year. We furthermore inspected that the operating procedures are accessible to all relevant employees.	No exceptions noted.

Control objective 6:

People controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
6.1	**Screening** *Background verification checks on all candidates to become personnel shall be carried out prior to joining the organisation and on an ongoing basis, take into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.* IT Relation performs screening of its potential candidates which includes obtaining clean criminal records on all employees employed by IT Relation. All employees are obligated to continuously supply a clean criminal record during their employment, and such criminal record is obtained by IT Relation every third year of employment.	We inquired Management regarding the procedures/control activities performed. We inspected that an HR process is in place to ensure that criminal records are presented before employment starts for both employees and external consultants and every third year of employment. From samples of new hires, we inspected that criminal records have been acquired before employment start.	No exceptions noted.
6.2	**Terms and conditions of employment** *The employment contractual agreements shall state the personnel's and the organisation's responsibilities for information security.* IT Relation has established terms and conditions of employment as part of the employment agreement between an employee and IT Relation. These include expectations of compliance with applicable information security initiatives.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation runs introductory courses for new employees during which terms and conditions of employment are included.	No exceptions noted.

Control objective 6:
People controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
6.3	**Information security awareness, education and training** *Personnel of the organisation and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organisation's information security policy, topic-specific policies and procedures, as relevant for their job function.* IT Relation performs various security awareness initiatives continuously based on an annual wheel and ad-hoc trending security threats in the world. IT Relation performs simulations of phishing attempts and other breaching attempts to increase employees' hand-on experience with actual breaching attempts. Furthermore, all employees are required to familiarise themselves with applicable information security requirements and the Information Security Policy.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation performs annual security awareness initiatives and performs information security campaigns regularly. By inspection, we verified, that employees have been introduced to the Information Security Policy.	No exceptions noted.
6.5	**Responsibilities after termination or change of employment** *Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.* IT Relation communicates information security responsibilities which remain valid after termination or change of employment. This includes obtaining written confirmation that the terminated employee understands their continued obligation.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation obtains a written confirmation of continued obligation after employment from terminated employees.	No exceptions noted.

Control objective 6:
People controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
6.6	**Confidentiality or non-disclosure agreements** *Confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.* IT Relation establishes confidentiality agreements with its employees as part of the initial, contractual employment agreements. Furthermore, some employees might be subject to additional confidentiality or non-disclosure agreement during their employment if required by customers.	We inquired Management regarding the procedures/control activities performed. By inspection of random samples, we verified that a non-disclosure agreement is signed as part of new employments.	No exceptions noted.
6.7	**Remote working** *Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organisation's premises.* IT Relation has established and implemented security measures for personnel working remotely and to ensure the information security level is adequate similar to when employees are working from the offices. This includes, among other things, establishing VPN connections and ensuring that all sensitive work is performed on virtual desktops.	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures have been implemented for personnel working remotely.	No exceptions noted.

Control objective 6:
People controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
6.8	**Information security event reporting** *The organisation shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.* IT Relation has established and provides a mechanism for personnel to report observed or suspected information security events. The procedure for utilising the mechanism is communicated to and made available to all employees.	We inquired Management regarding the procedures/control activities performed. We inspected that the incident management process has been communicated and made available to employees.	No exceptions noted.

Control objective 7:
Physical controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
7.2	**Physical entry** *Secure areas shall be protected by appropriate entry controls and access points.* IT Relation has established physical entry controls to secure areas which include identification cards, registration of visit and constant supervisions of approved and cleared employees.	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that IT Relation has implemented appropriate entry controls to protect physical facilities.	No exceptions noted.
7.3	**Securing offices, rooms and facilities** *Physical security for offices, rooms and facilities shall be designed and implemented.* IT Relation has implemented physical security in its offices which includes physical entry points accessible through personal ID cards and personal PIN codes, segregated security zones and CCTV.	We inspected that a formal physical access and security policy is maintained, reviewed and approved. We inspected that IT Relation has implemented appropriated entry controls to protect offices, rooms and facilities.	No exceptions noted.
7.4	**Physical security monitoring** *Premises shall be continuously monitored for unauthorised physical access.* IT Relation has established CCTV at entrances to both offices, data centres and other facilities processing sensitive information.	We inspected that CCTV is established at entrances to both offices, data centres and other facilities processing sensitive information.	No exceptions noted.
7.6	**Working in secure areas** *Security measures for working in secure areas shall be designed and implemented.* IT Relation has established procedures and guidelines for working in secure areas to ensure that performing work does not endanger employees and information assets.	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures have been established to secure employees and information assets.	No exceptions noted.

Control objective 7:
Physical controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
7.7	**Clear desk and clear screen** *Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.* IT Relation has established a clear desk and clear screen policy ensuring that sensitive information is not left unattended at the office and that screens and endpoints are locked whenever they are left unattended.	We inquired Management regarding the procedures/control activities performed. We inspected that a clear desk and clear screen policy has been implemented.	No exceptions noted.
7.8	**Equipment siting and protection** *Equipment shall be sited securely and protected.* IT Relation has a policy to ensure the protection of critical equipment.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation has established guidelines on the protection against fire, water and heat. We furthermore inspected that IT Relation has obtained an audit report from a subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	No exceptions noted.
7.9	**Security of assets off-premises** *Off-site assets shall be protected.* IT Relation has established and communicated rules for how assets should be protected and handled when taken off-premises.	We inquired Management regarding the procedures/control activities performed. We inspected 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 exceptions noted.

Control objective 7:
Physical controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
7.10	**Storage media** *Storage media shall be managed through their life cycle of acquisition, use, transportation and disposal in accordance with the organisation's classification scheme and handling requirements.* IT Relation has established and implemented policies and procedures for handling storage media throughout their life cycle.	We inquired Management regarding the procedures/control activities performed. By inspection, we verified that IT Relation has implemented formalised procedures for handling storage media throughout their life cycle.	No exceptions noted.
7.11	**Supporting utilities** *Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.* IT Relation ensures that all equipment owned by IT Relation is maintained as per the manufacturer's specification. Furthermore, IT Relation ensures that its partners do the same.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation has established a fully redundant infrastructure with individual backup.	No exceptions noted.
7.13	**Equipment maintenance** *Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.* IT Relation ensures to maintain equipment as specified by the manufacturer.	We inquired Management regarding the procedures/control activities performed. We inspected that relevant security measures are implemented to ensure maintenance of equipment.	No exceptions noted.

Control objective 7:
Physical controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
7.14	**Secure disposal or re-use of equipment** *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 has implemented guidelines for disposal or re-use of equipment, ensuring that if storage media is disposed of it is done through a certified vendor to ensure its destruction.	We inspected that IT Relation has implemented procedures on secure disposal or re-use of equipment. We inspected that disposal and re-use of equipment is handled through a certified vendor.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.1	**User end point devices** *Information stored on, processed by or accessible via user end point devices shall be protected.* IT Relation has implemented various security policies for its user end points ensuring that they are adequately protected. This includes, among other things, remote wiping capabilities of hard disk, malware protection, etc.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation has implemented a user end point device policy.	No exceptions noted.
8.2	**Privileged access rights** *The allocation and use of privileged access rights shall be restricted and managed.* IT Relation has a policy for allocation and restriction of users with privileged access. All users with privileged access have a dedicated user for the privileged access, and the privileged user access list is audited on a quarterly basis.	We inquired Management regarding the procedures/control activities performed. We inspected that IT Relation has established formalised procedures for privileged user administration. We inspected that privileged access rights granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior. Furthermore, we inspected that privileged user access rights are reviewed quarterly.	No exceptions noted.
8.3	**Information access restriction** *Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.* IT Relation has a policy of limiting access to systems and applications to employees who have a work-related need.	We inquired Management regarding the procedures/control activities performed. We inspected that a policy of limiting access to systems and applications to employees who have a work-related need has been implemented.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.5	**Secure authentication** *Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.* IT Relation has established secure authentication technologies to sensitive information which, among other things, include multi-factor authentication.	We inspected that a formal access control policy defining allowed technical solutions for authentication is maintained. We inspected that the access control policy has been reviewed and approved. We inspected that applications and systems in scope enforce secure log-on procedures.	No exceptions noted.
8.6	**Capacity management** *The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.* IT Relation has 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 capacity, to ensure that future capacity requirements are met.	We inquired Management regarding the procedures/control activities performed. We inspected that reports on production environment operations at IT Relation are sent to customers each month. We furthermore inspected that the capacity of production systems at IT Relation is monitored to ensure that future capacity requirements are met.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.7	**Protection against malware** *Protection against malware shall be implemented and supported by appropriate user awareness.* IT Relation has implemented procedures for ensuring working antivirus software on all applicable systems. The antivirus software is monitored. Protection against malware is supported with user awareness through IT Relation's security awareness platform, granting knowledge on malware defence to employees.	We inquired regarding the procedures/control activities performed. By inspection of random samples, we verified that antivirus software has been installed on all applicable systems and that antivirus software is monitored. Furthermore, we inspected that user awareness initiatives about antivirus software and malware defence have been established for employees.	No exceptions noted.
8.8	**Management of technical vulnerabilities** *Information about technical vulnerabilities of information systems in use shall be obtained, the organisation's exposure to such vulnerabilities should be evaluated and appropriate measures should be taken.* IT Relation has a procedure for continuously assessing vulnerabilities that are reported and assessing their criticality against multiple sources in connection with the services provided by IT Relation.	We inquired regarding the procedures/control activities performed. By inspection using random samples, we noted that technical vulnerabilities of information systems are obtained in a timely fashion and evaluated, and appropriate measures taken to address the associated risk. Furthermore, we inspected that critical vulnerabilities are communicated to all relevant stakeholders.	No exceptions noted.
8.9	**Configuration management** *The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.* IT Relation has established processes and procedures for configuration management to ensure that changes to configuration items are handled and documented properly.	We inquired Management regarding the procedures/control activities performed. We inspected that resources are monitored and adjusted in line with the current procedures for configuration management.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.10	**Information deletion** *Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.* IT Relation has established procedures for information deletion to ensure that no data is stored longer than required by regulative or business requirement.	We inquired Management regarding the procedures/control activities performed. We inspected that information is deleted in line with IT Relation's procedures.	No exceptions noted.
8.13	**Information backup** *Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.* IT Relation performs backup in accordance with IT Relation's best practice or customers' business requirements. The backup jobs are monitored to ensure their continuous operation. Annually, a recovery test is initiated by IT Relation.	We inquired Management regarding the procedures/control activities performed. We inspected that requirements regarding backup have been established in the contract with sub-contractors that provide services where backup is relevant. We inspected that a full restore test of IT environments has been performed.	No exceptions noted.
8.14	**Redundancy of information processing facilities** *Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.* IT Relation has redundancy in its own information processing facilities and has the possibility to provide redundancy if the customer has these requirements.	We inquired Management regarding the procedures/control activities performed. We inspected that redundancy has been implemented on IT Relation's information processing facilities and on customer environments according to signed customer contracts.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.15	**Logging** *Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.* IT Relation performs Security Information and Event Management (SIEM) on its own systems and if the customer has these requirements. IT Relation records logs for different systems at different security levels. For the SIEM system, the segregation of duty is full. Employees who have access to delete log data have no access to customer systems and IT Relation systems. All access to customer systems is logged in the access 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.	We inquired Management regarding the procedures/control activities performed. We inspected that logging of user activities, exceptions, faults and information security events has been configured. We inspected that all user access activity to customer data is logged. Furthermore, we inspected that sufficient segregation of duties have been implemented to log systems.	No exceptions noted.
8.16	**Monitoring activities** *Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.* IT Relation has implemented a monitoring system which ensures that the customers' systems are running, and any anomalous behaviour is alerted through the monitoring system. The system is monitored 24/7.	We inquired Management regarding the procedures/control activities performed. We inspected that a monitoring system has been implemented and that the system is monitored 24/7.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.17	**Clock synchronisation** *The clocks of information processing systems used by the organisation shall be synchronised to approved time sources.* IT Relation has synchronised all relevant information processing systems to a single reference time source.	We inquired regarding the procedures/control activities performed. We inspected that IT Relation has established a reference time source for clock synchronisation of all relevant information processing systems.	No exceptions noted.
8.19	**Installation of software on operational system** *Procedures and measures shall be in place to securely manage software installation on operational systems.* IT Relation has defined a set of standard implementation descriptions. These systems are allowed on customer systems.	We inquired Management regarding the procedures/control activities performed. We inspected that software installation on operational systems are managed appropriately and according to current procedures.	No exceptions noted.
8.20	**Networks security** *Networks and network devices shall be secured, 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 inquired regarding the procedures/control activities performed. By inspection, we 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 exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.22	**Segregation of networks** *Groups of information services, users and information systems shall be segregated in the organisation's 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 inquired Management regarding the procedures/control activities performed. We inspected the technical security architecture and, by inspection of random samples, we 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 exceptions noted.
8.23	**Web filtering** *Access to external websites shall be managed to reduce exposure to malicious content.* IT Relation has implemented web filtering measures which include protection and reduction of exposure to malicious content.	We inquired Management regarding the procedures/control activities performed. We inspected that web filtering measures have been implemented.	No exceptions noted.
8.24	**Use of cryptography** *Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.* IT Relation has established policies on the use of cryptography which include rules of usage, selection of cryptographic technique, implementation, maintenance and disposal.	We inquired Management regarding the procedures/control activities performed. We inspected that appropriate use of cryptography and cryptographic key management have been established.	No exceptions noted.

Control objective 8:
Technological controls

Nr.	IT Relation's control activity	Tests performed by PwC	Result of PwC's tests
8.32	**Change management** *Changes to information processing facilities and information systems shall be subject to change management procedures.* IT Relation has established and implemented a change management process that ensures that all changes to information systems in production environments are subject to change management, which ensures that changes do not unnecessarily affect each other and that change fall back plans are in place.	We inquired regarding the procedures/control activities performed. We inspected 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 exceptions noted.