www.pwc.dk

The following is a translation of a Danish original document. Please note that the English translation is provided for convenience only. In case of any discrepancy, the Danish version shall prevail.

Itadel

ISAE 3402 Independent Service Auditor's Assurance Report on IT General Controls relating to financial reporting for Itadel's hosting services

January 2019

Contents

1. Assertion by the service organisation

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

(a) The accompanying description in section 2 fairly presents the IT General Controls in relation to hosting services for Customers throughout the period 1 January 2018 to 31 December 2018. The criteria used in making this assertion were that the accompanying description:

(i) Presents how the Customers' solutions was designed and implemented, including:

- The types of services provided, including, as appropriate, classes of transactions processed
- The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers
- Relevant control objectives and controls designed to achieve those objectives
- Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions

(ii) Includes relevant details of changes to the service organisation's system during the period 1 January 2018 to 31 December 2018

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

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period 1 January 2018 to 31 December 2018. The criteria used in making this assertion were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period 1 January 2018 to 31 December 2018.

Aarhus, 16 January 2018

Nils Lau Frederiksen
Information Security Manager, Itadel

2. Itadel's description of IT General Controls relating to financial reporting for Itadel's hosting services

Vision
We want to be recognised as the IT outsourcing partner delivering highest value and best service for our customers through delivery of secure and scalable solutions.

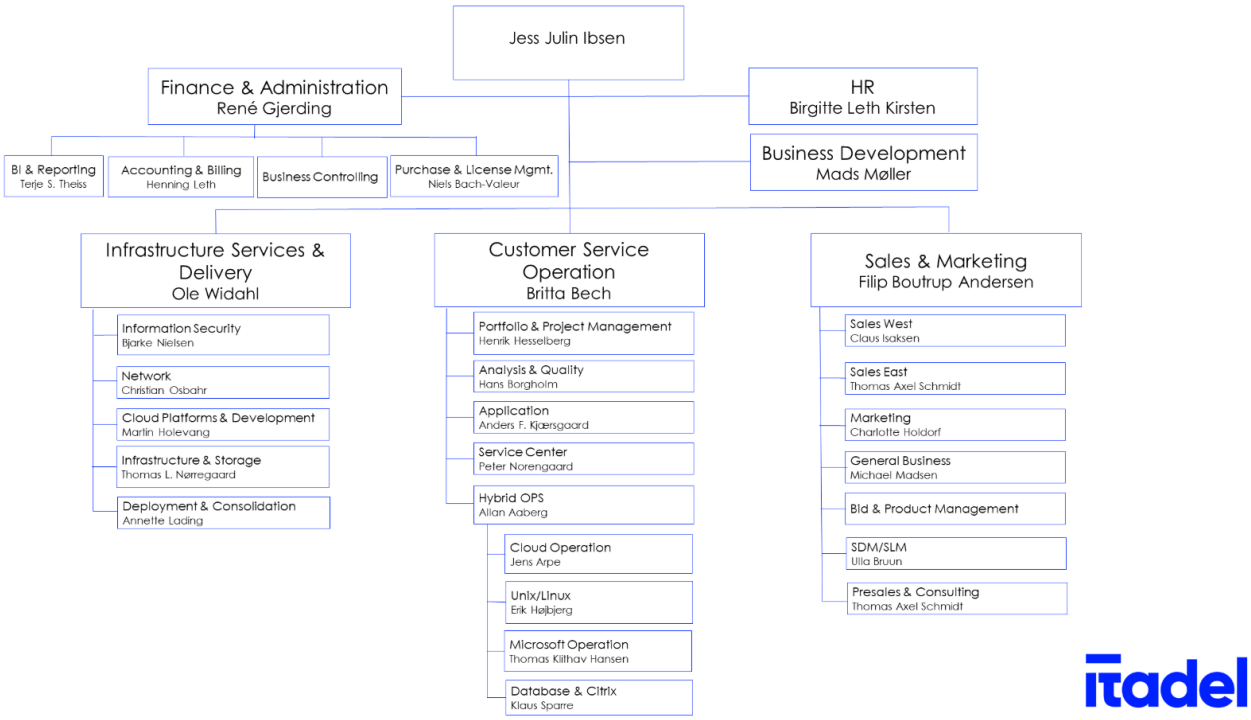
Mission
- Our customers experience that we understand their business, take responsibility and provide a high level of service
- Our customers have minimised risks as we deliver secure IT operations and data protection
- Our customers can focus on core business because we release customers' resources
- We help our customers with digital transformation
- We make it easy for our customers doing business with us.

Our DNA
- We focus on informality and establishing a good rapport with our clients. At the same time, we are approachable and provide easy access to highly educated and skilled SMEs.
- We do not produce documentation purely for the sake of documentation – we do so, only when it creates value for the client.
- As we strive to always be flexible, we work with processes to the extent our clients consider such work value adding.
- We have strong professional skills as well as comprehensive operating experience across systems and solutions.
- We started out as a small operation and have now grown to be a successful business; during this process, we have accumulated considerable experience and developed a range of services in close cooperation with our clients.
- We are action-oriented and committed to providing solutions that match the needs of our clients perfectly – we always put our clients first.
- Our shared 'client ownership' principle implies shared best practice, a high level of knowledge sharing and disciplined operating documentation across the organisation.

Organisational structure
Itadel currently employ 300 people; 200 of these are technical personnel. We operate six data centres in Denmark, some of which (the most recently built) have been set up as software-defined data centres (SDDC) offering a standard solution that is based on two centres.

Itadel's organisational structure is based on the most significant areas of operation – i.e. functional areas, which either support or provide professional hosting services, cf. the organisational chart presented below.

Organizational Chart

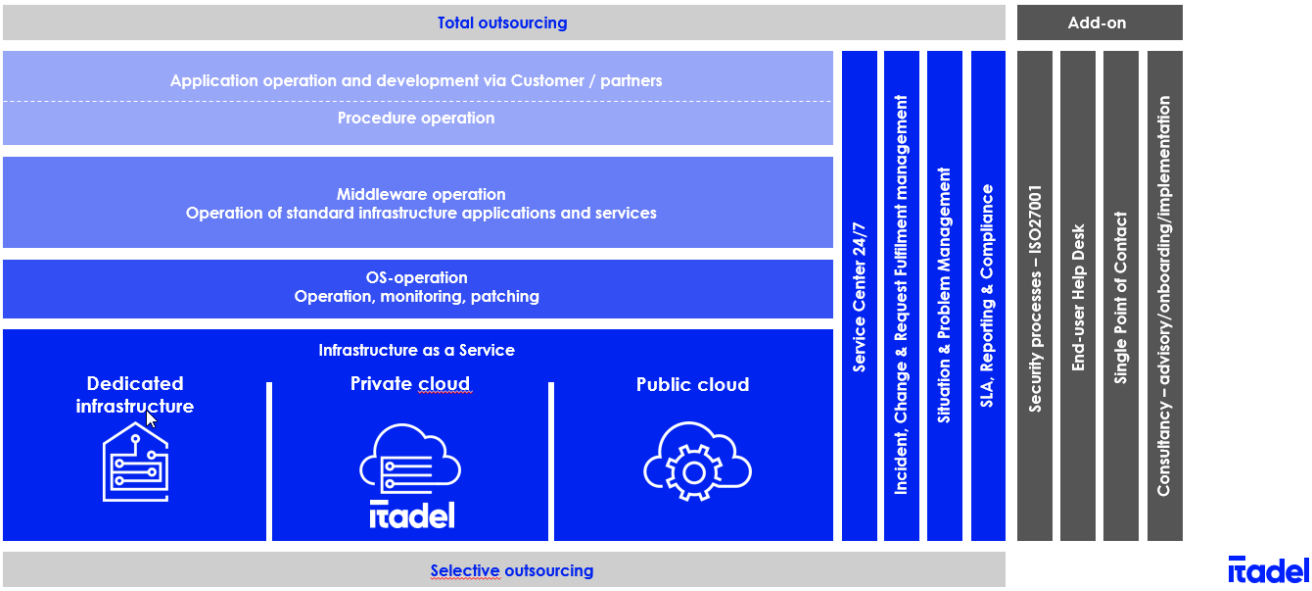


Competencies and staffing
Generally, our technicians are allocated to system-specific work – and not to a particular client.
Their competencies, certifications and experience are mapped in a 'knowledge map', allowing us to:

- assemble high-performance teams
- ensure that incoming tickets are assigned to the right technicians or team from the outset; as a result, tickets are handled quickly and efficiently
- make the requisite competencies available 24-7.

We furthermore place great emphasis on continuous training and education to make sure that experience in and knowledge of our clients and systems are passed on and communicated in an effective and efficient manner.

Operating concept and business-critical services
Itadel provides operation of IT systems to private as well as public enterprises. Our core services include solutions based on 'infrastructure as a service', OS operation, middleware operation as well as operation of procedures and applications. These services are described in detail in the statement of deliverables.



Infrastructure as a service

- Servers, storage, backup, network, load balancers and firewalls
- A fully secure data centre solution with installed access control, fire prevention equipment, anti-theft alarms, temperature control (alarm) and a diesel generator for emergency power purposes. Alarms are sent to the service desk function and selected third-party suppliers (e.g. the fire brigade)
- Direct internet access to TDC's backbone
- Enterprise components in a redundant set-up
- Our fully scalable cloud solution includes a self-service portal for the creation/deletion of servers, the allocation of storage space, and the set-up of firewalls and load balancers.

OS operations

- Installation, operation, backup and patching of basic OS solutions
- Anti-virus
- Monitoring of servers and OS 24-7 as well as access to a service desk function
- OS-related software licences, backup and anti-virus.

Middleware operation

- Full responsibility for the operation of standard server applications (e.g. Citrix, Exchange, IIS, Apache, SQL, Oracle)
- The use of Itadel's best practice principles in the context of standard server applications
- Backup and restore management in relation to middleware applications and associated data
- Patching (we always adhere to the software developer's guidelines on security vulnerability patching)
- 24-7 monitoring of applications and access to a service desk function.

Operation of procedures

- Operation of customer-specific applications on the basis of defined procedures
- The client, third parties and Itadel cooperate closely to define procedures (procedures may range from the simple restarting of services to release management at the application layer)
- 24-7 monitoring of applications and access to a service desk function
- Operating experience is gathered and documented.

Application operations

- We furthermore offer application operation services via end-user helpdesk functions and SPOC.

Description of IT general controls

Implemented controls

Itadel is an ISO 27001-certified enterprise; the selected control objectives and a brief general description of implemented ISO 27002 controls are presented below. The complete list is included in Itadel's "Statement of Applicability". In organisational terms, responsibility for certification and ISO 27002 controls rests with the Information Security function.

Risk management

In Itadel, risk management has been implemented in accordance with ISO 27001, which requires a risk-based approach to security. Itadel has therefore incorporated risk management into its processes, for example the Change Management process. The following table shows what preventive and corrective measures Itadel has implemented:

	Preventive measures	**Detective measures**
Organisational measures	• Policies, procedures and instructions • Awareness • Change management • Technical best practices • Operational acceptance test • Compliance controls • Supplier contracts • Service- and support agreements • CMDB/system documentation.	• Contingency plans • Disaster recovery procedures • Procedure for major incidents • Incident management • Problem management.
Physical and technical measures	• Firewalls • Antivirus • Alarm systems • Monitoring • Test environments • Intrusion prevention • Redundancy • Identity management • Clusters • UPS.	• Logging • Standby equipment • Standby site • Backup/restore • Server snapshots • Virtualisation • Fire extinguishers • Emergency power.

Information security policies

Itadel has implemented security policies that reflects security strategies and objectives.

The management team of Itadel has prepared an information security policy that sets out clear IT security objectives. The policy is subject to annual review. Information security is managed by Itadel's "Information Security Management System" (ISMS). The ISMS contains detailed information, on among other things, password management and auditing at Itadel as well as guidelines on the security level of: OS, servers, workstations, network and storage. Itadel's ISMS also contains information on the requirements for segregation of duties and user management with respect to Itadel's operations-critical systems as well as shared infrastructure and client solutions.

Organisation of information security

Responsibility for adherence to the information security policy and guidelines contained in the ISMS lies with the individual department management teams. The security work of the department management team is supported by a dedicated security function under the management of Itadel's IT security manager.

At Itadel, responsibility for information security is carried out through the classification of processes, systems and data, including the determination of organisational ownership. In the context of the above, segregation of duties is taken into consideration.

Itadel has implemented a procedure for the communication with local authorities; said procedure has been anchored in the Finance and Human Resources functions. Communication with special-interest groups is handled by the relevant functions, i.e. the functions to which the communication pertains.

Itadel has prepared a policy for information security management in connection with project execution. The purpose of this policy is to ensure that projects (internal as well as external) do not present a risk for Itadel and Itadel's clients.

Itadel places great emphasis on the management of mobile devices and teleworking; the rules applicable to mobile devices and teleworking are stated in Itadel's information security manual – "General rules for information security at Itadel". A copy of the manual is provided to all new hires in connection with their receipt of an employment contract.

Human resources security
Itadel has defined processes for employment, inter-company rotation and termination of employees' contracts. All employees are subject to screening as part of the recruitment process. Employees who will be accessing customer-specific data or other sensitive information as part of their job function are security-cleared. All employees are informed of the applicable security processes, procedures and instructions as part of the on-boarding process. The processes are anchored in and managed centrally by the Human Resources function.

Itadel has defined and documented a disciplinary process, which enters into force upon a breach of security.

On termination of employment, employees are informed of their obligations, including those that are to be honoured after their exit. Equipment received in the course of the employment is to be returned to Itadel, and access rights will be revoked.

Asset management
Itadel has implemented ownership of information assets with respect to shared infrastructure and client environments. The ownership of each individual asset is recorded and tracked in a central register. The designated owner of an asset is responsible for the full life cycle of the asset; one of the tasks of the owner is to classify the asset based on an assessment of confidentiality, integrity and availability (CIA). Employees receive information on what is considered 'acceptable use' of equipment. 'Acceptable use' is specified in detail in the information security manual. The return of assets by employees takes place in accordance with the process for termination of employment.

When no longer in use, equipment containing data is destroyed in accordance with relevant procedures. In the entire process from dismantling to destruction, equipment is protected against unauthorised use.

Access control
Itadel has established access control at several levels to reduce the risk of unauthorised individuals gaining access to systems and data. Physical and logical access control measures have been established. Access control is supported by processes and controls in connection with the assignment and maintenance of access rights to systems and data.

Users are created, managed and deleted in accordance with the applicable security policy; privileges and access rights are granted based on a work-related need. Secure log-on procedures have been effected in password policies, which have been implemented in accordance with the recommendations of established system suppliers.

Itadel performs periodic reviews of users, rights and access. Discrepancies are investigated and rectified without undue delay.

Encryption (cryptography)
The classification of data/information determines the stringency of encryption-related requirements.

In accordance with Itadel's information security manual, sensitive data are to be protected by means of encryption. Examples of the above are: equipment made available to employees and backup of client data.

Physical and environmental security
Itadel ensures physical security through a number of implemented security measures, including a 'clear desk and screen' policy and access control at locations and data centres; to avoid trespassing, all employees are to carry visible ID cards. People without proper authorisation who have business at Itadel's locations are received by the staff in the reception who handle registration and issue a visitor's card. All guests are escorted by the employees with whom they have made an agreement.

Itadel has implemented procedures for the use of loading/unloading areas, equipment maintenance, the securing of wiring as well as the reuse and destruction of equipment. The procedures are detailed in "Management of information assets".

Itadel's data centres are protected against physical threats such as fire, water, heat and the failure of supply lines, including electricity supply lines. We have established a power supply with backup (battery-driven and through generators), fire protection, fire alarms and fire-extinguishing equipment along with monitoring of the data centre infrastructure. All among data centres shared infrastructure devices have been configured dimensionally with fully redundant systems; each system is backed up separately. Network connections from the data centres are also fully redundant.

Operational security
Itadel has documented a number of procedures and instructions that support stable and secure operations; this documentation is contained in the ISMS. The procedures etc. are based on our business processes and controls, which again are based on ITIL best practice. Among other things, we have implemented change management, incident management and capacity management processes. Vulnerabilities are prevented through e.g. patch management, anti-malware systems and 24-hour staffed monitoring. Itadel has implemented backup to prevent data loss etc. in connection with the interruption of operations. The backup is subject to regular testing; test intervals are determined based on the data classification. Vulnerabilities identified in connection with e.g. an information security incident are registered, and suitable preventive/remedial measures are taken.

Communications security
Network access is divided into technical and non-technical access and is granted in accordance with employees' work-related needs. Access to infrastructure and operational systems is isolated on a technical network. To prevent unauthorised access to the technical network, two-factor authentication via password and RSA tokens has been implemented.

Itadel's operational information and communication are centrally anchored in the company's internal operating portal. The portal contains all significant guidelines, processes and tools associated with the operation of Itadel's infrastructure, internal systems and client-specific solutions.

Itadel makes use of non-disclosure agreements where this is considered necessary to protect sensitive and confidential data.

System acquisition, development and maintenance
Itadel has implemented a policy on information security in connection with project execution. This policy and the implemented change management process are instrumental in ensuring that the requisite risk assessments are performed. This applies to the full life cycle of all of Itadel's systems and solutions.

In the operating phase, risk management is an explicit part of the implemented change management system. In the system, all major changes to operating systems are to be documented, assessed, adjusted (if relevant), approved, planned and executed in accordance with defined routines and procedures. As far as the client finds it necessary to depart from agreed security standards/best practice, an agreement to this effect is to be made between Itadel and the client. The agreement is to be documented in a risk letter.

Itadel's internal systems have an infrastructure that is separated from the infrastructure of client systems. The systems are operated according to the same service model as that described in a standard delivery description. The service model addresses risks associated with change management, access control, backup, supporting infrastructure redundancy, etc.

Supplier relationships
Services from significant service suppliers are subject to the information security requirements described in "Information security policies". Itadel has appointed an in-house resource to assume responsibility for the entire life cycle, such as the classification of suppliers, the drafting of non-disclosure agreements and the execution of audits.

Information-security incident management
Itadel's information security function is responsible for preparing reports on and managing security-related incidents and vulnerabilities. Security incidents are documented and investigated in accordance with formalised procedures – and if they are deemed to constitute a significant risk, relevant activities are initiated. At regular intervals, Itadel's management team receives updates on progress made in the area.

Itadel performs systematic risk assessments of internal critical assets, such as key infrastructure elements, systems and processes, which support operations. These risk assessments are performed based on the parameters of availability, confidentiality and integrity.

Information security aspects of business continuity management
Itadel has taken the necessary precautions and established contingency plans to re-establish operational systems in case of a disaster scenario. These precautions include the establishment of a contingency organisation, including rooms and access, guidelines to be followed by the contingency management team, staffing, lists of systems, re-establishment/contingency operation, other activities, communication and contact lists, etc.

Compliance
Itadel has implemented procedures for monitoring and evaluation of changes to relevant legislation.

Itadel has implemented procedures for the approval, acquisition and use of software. We cooperate with our software suppliers when it comes to licence management and statement of products. Depending on the type of licence (licence held/leased), information is provided to the accounting function on a continuous basis.

Itadel has implemented a portal, which serves as a list of key information and systems. The portal is used by Itadel's employees to execute work on a day-to-day basis.

Data are treated in accordance with the associated classification and the principle of segregation of duties; this also applies to personal data. Itadel's information security manual includes guidelines on the security levels applicable to equipment provided to employees.

Itadel is ISO27000 certified. Therefore, a review of the ISMS is performed at least once a year. Furthermore, a number of independent auditor's reports, a general ISAE 3042 report, a general ISAE 3000 report, which from 2018 is in accordance with the European General Data Protection Regulation (GDPR), as well as a number of client-specific reports are prepared. Procedures and policies are revised as needed. Procedures and policies are currently being heavily revised due to the now effective split between TDC and Itadel in the winter of 2017.

This description has been prepared exclusively for companies that – based on the standard delivery document – have entered into an agreement with Itadel concerning service delivery, and their auditors, and it should not be used for any other purpose.

Improvements
In 2018, Itadel has implemented the following improvements to the level of security:

Month	Measures
June 2018	Physical RSA tokens for multi-factor authentication have been replaced with MFA application for smartphones.
August 2018	Four new employees have been taken on in Information Security, increasing the number of information security staff to 7 FTE.
September 2018	Itadel has educated 14 of its own employees to internal ISO27001 auditors.

3. Service auditor's assurance report

To the Management of Itadel, Itadel's customers of Itadel's hosting services and their auditors

Scope
We have been engaged to report on Itadel's description in section 2 of IT General Controls in relation to Itadel's hosting services, cf. the standard delivery document version 3.3, (below referred to as operational services) (the system) for processing customers' transactions throughout the period 1 January 2018 to 31 December 2018 and on the design and operation of controls related to the control objectives stated in the description at physical locations in Denmark.

Itadel's responsibilities
Itadel is responsible for preparing the description and accompanying assertion, including for the completeness, accuracy and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

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

PricewaterhouseCoopers applies the International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control, including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

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

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we considered necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified by the service organisation and described in section 1.

We believe that the evidence we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organisation
Itadel'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 IT General Controls that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion
Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 1. In our opinion, in all material aspects:

(a) The description fairly presents the operational services as designed and implemented at physical locations in Denmark throughout the period 1 January 2018 to 31 December 2018.

(b) The controls related to the control objectives stated in the description were suitably designed throughout the period 1 January 2018 to 31 December 2018.

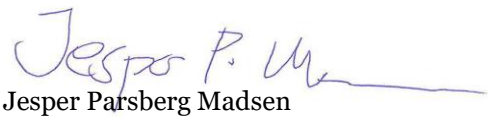
(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives were achieved, operated effectively throughout the period 1 January 2018 to 31 December 2018.

Please note that our opinion alone covers hosting services under Itadel's applicable SoA and security policy; customer-specific requirements and other matters are not included. In so far as a customer requests a statement on such requirements and matters, said customer must enter into a separate agreement with Itadel.

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 Itadel's hosting services and their auditors who have a sufficient understanding to consider these along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatements in customers financial statements in the period 1 January 2018 to 31 December 2018.

Aarhus, 16 January 2019
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab



Jesper Parsberg Madsen
State-Authorised Public Accountant

Iraj Bastar
Senior Manager

4. Control objectives, controls, tests and related findings

A.5 Control objective: Information security policies

Itadel's control activity	Control tests performed by PwC	Results of tests
5.1.1 Policies for information security *A set of policies for information security should be defined, approved by management, published and communicated to employees and relevant external parties.* The information security policy is documented and maintained through review at least once a year. The policy has been approved by Management. The information security policy has been made available to the employees via the intranet.	We have briefly discussed information security governance with Management. By inspection, we have observed that a Management-approved and up-to-date security policy is in place. By inspection, we have verified that the security policy is reviewed at least once a year.	No significant exceptions noted.
5.1.2 Review of policies for information security *The policies for information security should be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.* The organisational responsibility for information security is documented and implemented. Information security and related initiatives are handled by the operating organisation and supported by a dedicated security function, i.e. a staff function assisting the technical organisation.	We have briefly discussed information security governance with Management. By inspection, we have observed that the policies for information security are reviewed at planned intervals or in connection with significant changes.	During our audit of the policies, we have observed that policies in the ISMS system have not been updated annually. We have been informed that ISMS is undergoing restructuring, and all documents under ISMS are planned for review in Q1 2019. No further significant exceptions noted.

A.6 Control objective: Organisation of information security

Itadel's control activity	Control tests performed by PwC	Results of tests
6.1.1 Information security roles and responsibilities *All information security responsibilities should be defined and allocated.* The organisational responsibility for information security is documented and implemented. Information security and related initiatives are handled by the operating organisation and supported by a dedicated security function, i.e. a staff function assisting the technical organisation.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that the organisational areas of responsibility have been defined and allocated to relevant personnel. We have observed that information security and related initiatives are addressed by department managers and supported by staff functions.	No significant exceptions noted.
6.1.2 Segregation of duties *Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorised or unintentional modification or misuse of the organisation's assets.* The Management of Itadel has implemented policies and procedures to ensure satisfactory segregation of duties. Thus, development and operating activities and access to primary and secondary data are segregated unless employees are in need of elevated rights to perform their job function.	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have investigated whether the critical operating functions at Itadel have been appropriately segregated and whether primary and secondary operating data have been segregated.	No significant exceptions noted.
6.2.1 Mobile device policy *A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.* Itadel places great emphasis on governance of mobile devices and has set out rules in this particular area in its information security manual 'General rules on information security at Itadel'. A copy of the manual is provided to all new hires in conjunction with their employment contract.	With Management, we have briefly discussed procedures and guidelines to ensure adoption of security measures that manage the risks introduced by mobile devices. We have verified that procedures for the use of mobile equipment have been established.	No significant exceptions noted.
6.2.2 Teleworking *A policy and supporting security measures should be implemented to protect information accessed, processed or stored at teleworking sites.* Itadel has established guidelines to protect systems and data outside the corporate network. Furthermore, two-factor authentication has been enabled to ensure that employees are not able to access data from teleworking sites unless necessary in order for them to perform their job function.	We have briefly discussed the procedures/control activities performed with Management. We have briefly discussed procedures and guidelines on teleworking sites with Management. By inspection, we have observed that guidelines have been established on compliance with security rules in connection with the use of teleworking sites. It is our assessment that access control through a two-factor VPN connection complies with the security requirements laid down in the Danish Data Protection Act.	No significant exceptions noted.

A.6 Control objective: Organisation of information security

Itadel's control activity	Control tests performed by PwC	Results of tests
	We have observed that the security statement signed by Itadel's new hires includes the mentioned guidelines on teleworking sites, including the prohibition on downloading sensitive personal data on computers used at teleworking sites.	

A.7 Control objective: Human resource security

Itadel's control activity	Control tests performed by PwC	Results of tests
7.1.2 Terms and conditions of employment *The contractual agreements with employees and contractors should state their and the organisation's responsibilities for information security.* Itadel has laid down rules on confidentiality agreements that employees are to sign at the time of employment and confidentiality agreements that external consultants are to sign prior to starting work.	We have briefly discussed the procedures/control activities performed with Management. Using random samples, we have observed that confidentiality agreements are used in accordance with the guidelines, including: • that employees sign confidentiality agreements at the time of employment • that external consultants sign confidentiality agreements prior to starting work.	No significant exceptions noted.
7.2.1 Management responsibilities *Management should require all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.* Through agreements, Itadel has set out requirements for employees and suppliers that ensure that the policies and procedures established by the organisation are adhered to.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that signed contracts are in place for employees and suppliers with a view to ensuring that the information security requirements of the organisation are met.	No significant exceptions noted.
7.2.2 Information security awareness, education and training *All employees of the organisation and, where relevant, contractors should receive appropriate awareness education and training and regular updates in organisational policies and procedures, as relevant for their job function.* Itadel introduces its employees to information security at the time of employment. In supplier agreements, Itadel has set out information security requirements that are in line with the policies and procedures established by the organisation.	We have briefly discussed the procedures/control activities performed with Management. We have observed that Itadel runs introductory courses for new employees during which information security requirements are explained. We have furthermore observed that employees are enrolled in mandatory training programmes at regular intervals for the purpose of ensuring compliance with the security requirements of the organisation. We have observed that agreements with suppliers have been concluded to ensure that the information security requirements of the organisation are met.	No significant exceptions noted.

A.7 Control objective: Human resource security

Itadel's control activity	Control tests performed by PwC	Results of tests
7.2.3 Disciplinary process *A formal and communicated disciplinary process should be in place to take action against employees who have committed an information security breach.* Itadel has established guidelines ensuring that a disciplinary process is initiated if an employee has committed an information security breach.	We have briefly discussed the procedures/control activities performed with Management. With Management, we have briefly discussed the guidelines on the disciplinary process in place to take action against employees who have committed an information security breach. Using random samples, we have observed that the guidelines on breach of information security have been communicated to employees in connection with the signing of non-disclosure agreements.	No significant exceptions noted.
7.3.1 Termination and change of employment *Information security responsibilities and duties that remain valid after termination or change of employment should be defined, communicated to the employee or contractor and enforced.* Itadel ensures that, following termination or change of employee contracts, user rights to operating systems, networks, databases, etc. are revoked in a timely manner.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that employees' access rights to operating systems, networks, databases, etc. are revoked in connection with the termination of employment.	No significant exceptions noted.

A.8 Control objective: Asset management

Itadel's control activity	Control tests performed by PwC	Results of tests
8.1.1 Inventory of assets *Assets associated with information and information-processing facilities should be identified, and an inventory of these assets should be drawn up and maintained.* Itadel has drawn up an inventory of critical assets and established procedures to ensure continuous maintenance of said inventory.	We have briefly discussed the procedures/control activities performed with Management. We have observed that adequate controls are in place to ensure documentation and maintenance of the inventory of assets.	No significant exceptions noted.
8.3.2 Disposal of media *Media should be disposed of securely when no longer required, using formal procedures.* Itadel has drawn up guidelines on the disposal, sale, destruction, repair and servicing of IT equipment.	We have briefly discussed the procedures/control activities performed with Management. We have verified that Itadel has implemented formalised procedures for the processing and destruction of input and output data material. We have verified that the controls to ensure validation of input data material are performed and that the guidelines on secure destruction of output data material are followed.	No significant exceptions noted.

A.9 Control objective: Access control

Itadel's control activity	Control tests performed by PwC	Results of tests
9.1.1 Access control policy *An access control policy should be established, documented and reviewed based on business and information security requirements.* Itadel has established guidelines ensuring that employees are assigned rights based on their job function and in compliance with the information security requirements of the organisation. Customers are provided with individual VLANs under which the customers' solutions are separated into a range of secure zones that are part of the security architecture.	We have briefly discussed the procedures/control activities performed with Management. We have observed that guidelines on access controls have been established, including through remote access, at the location and for suppliers.	No significant exceptions noted.
9.1.2 Access to networks and network services *Users should only be provided with access to the network and network services that they have been specifically authorised to use.* Itadel reviews all access requests for new and existing users in relation to applications, databases and data files to ensure compliance with Itadel's policies; this ensures that rights are granted on the basis of users' job function, are approved and created correctly in the systems.	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have reviewed selected servers and determined whether or not employees are created on each server/device and whether or not such creation is based on the employees' job function. We have observed that Itadel has documented which employees servicing a particular customer are authorised to make changes to these rights.	During our audit of Itadel's VPN access, we have observed that there is no requirement for the use of machine certificates. Access via VPN requires user name, password and two-factor authentication. You can thus access Itadel's internal environment from any client. There is no validation of the applications used on the connected client. We have been informed that Itadel is working to implement machine certificates for VPN connections in 2019. No further significant exceptions noted.
9.2.1 User registration and de-registration *A formal user registration and de-registration process should be implemented to enable assignment of access rights.* Access to operating systems, networks, databases, etc. is protected by passwords that comply with applicable security requirements with respect to length, complexity, maximum age, etc. Furthermore, users are locked following several failed login attempts. Passwords for customers' systems are created, managed and deleted from a central identity management system (IMS). The IMS assigns access codes on the basis of policies and roles.	We have briefly discussed the procedures/control activities performed with Management. We have observed that procedures for user administration have been established; by inspection of random samples, we have furthermore observed: • that, pursuant to applicable guidelines, follow-up on users' rights in operating environments is performed at regular intervals • that these rights are granted on the basis of users' job function By inspection of random samples, we have observed: • that passwords are used in accordance with applicable guidelines	No significant exceptions noted.

A.9 Control objective: Access control

Itadel's control activity	Control tests performed by PwC	Results of tests
	• that programmed controls are in place to enforce change of password at regular intervals • that controls established in relation to the IMS ensure secure high-quality passwords.	
9.2.2 User access provisioning *A formal user access provisioning process should be implemented to assign or revoke access rights for all user types to all systems and services.* Itadel has implemented processes that ensure that access rights are assigned based on users' job function. All authorisations at Itadel must be approved by the employee's immediate superior and include an access request justification. The authorisation procedures implemented at Itadel ensure that user creation and rights allocation are subject to written approval by an authorised person. At Itadel, all access rights are personal and treated confidentially, just as the identity of users is verified prior to authorisation being granted.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established formalised procedures for user administration and rights management. We have observed that authorisations granted at Itadel include an access request justification.	During auditing of user access assignment procedures, we have observed, at random sample testing, that there is insufficient documentation for system owner approval. No further significant exceptions noted.
9.2.3 Management of privileged access rights *The allocation and use of privileged access rights should be restricted and controlled.* Itadel has established formalised procedures that ensure that access rights, including privileged rights, are granted on the basis of users' job function. At Itadel, all user accounts are personal and treated confidentially, just as the identity of users is verified prior to authorisation being granted.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established formalised procedures for user administration and rights management and that these also apply to users with privileged rights. We have observed that authorisation granted to employees is accompanied by a justification of the level of access requested and an approval from the immediate superior. By inspection, we have observed that IT systems are subject to these procedures and control activities.	During our audit of the configuration of selected Windows servers and MSSQL databases related to administrator access, we have observed that there is no clear overview of the definition of responsibilities between the customer and Itadel in terms of setting up servers and databases related to administrator rights. We have observed that there are units without received risk letter, where the customer himself has administrator accesses. We have been informed that risk letters will be prepared in these cases to clarify the responsibilities in 2019. No further significant exceptions noted.

A.9 Control objective: Access control

Itadel's control activity	Control tests performed by PwC	Results of tests
9.2.4 Management of secret authentication information of users *The allocation of secret authentication information should be controlled through a formal management process.* Editing of network infrastructure and customer environments is exclusively performed by authorised personnel verified by two-factor authentication and AD groups.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established procedures that ensure that only authorised personnel verified by two-factor authentication and AD are able to make changes to the network infrastructure and customer environments. We have furthermore observed that all access to customer environments at Itadel is logged.	No significant exceptions noted.
9.2.5 Review of user access rights *Asset owners should review users' access rights at regular intervals.* Itadel reviews user IDs and rights for the purpose of ensuring that these are in accordance with users' job function. Discrepancies are investigated and resolved in a timely manner.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that user access rights are reassessed once every six months.	During the audit of the user administration procedures, we have been informed that there is currently no procedure for periodically evaluating users in AD. Furthermore, during the review of the periodic follow-up procedure for access by technicians, we have observed that there has been no quarterly review of technician access in accordance with Itadel's procedures. We have been informed that the audit will be reviewed and will be thoroughly checked after the next recertification round in January 2019. No further significant exceptions noted.
9.2.6 Removal or adjustment of access rights *The access rights of all employees and external users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.* Itadel ensures that, following termination or change of employee contracts, user rights to operating systems, networks, databases, etc. are revoked in a timely manner.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have investigated whether regular follow-up is performed on user rights in operating environments and whether these rights are granted based on users' job function.	No significant exceptions noted.
9.3.1 Use of secret authentication information *Users should be required to follow the organisation's practices in the use of secret authentication information.* Itadel has established appropriate procedures for data communication to reduce the risk of loss of integrity,	We have briefly discussed the procedures/control activities performed with Management. We have observed that Itadel has introduced controls ensuring the confidentiality of relevant information.	No significant exceptions noted.

A.9 Control objective: Access control

Itadel's control activity	Control tests performed by PwC	Results of tests
availability and confidentiality. Furthermore, the network has been segregated into a technical and administrative network as well as private networks pursuant to agreement with customers. Also, remote access via an external connection is managed through VPN using two-factor authentication.		
9.4.1 Information access restriction *Access to information and application system functions should be restricted in accordance with the access control policy.* Itadel has drawn up guidelines on authorisation management and control. Among other things, Itadel has ensured that control measures have been implemented in systems with a view to ascertaining that only authorised users are able to access personal data and that they are only able to perform the tasks for which they have authorisation. Itadel has implemented guidelines to ensure correct user creation and deletion.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has drawn up guidelines on authorisation management and control. We have observed that access to the systems at Itadel is granted on the basis of users' job functions.	No significant exceptions noted.
9.4.2 Secure log-on procedures *Where required by the access control policy, access to systems and applications should be controlled by a secure log-on procedure.* Itadel has drawn up guidelines on authorisation management and control. Among other things, Itadel has ensured that control measures have been implemented in systems with a view to ascertaining that only authorised users are able to access personal data and that they are only able to perform the tasks for which they have authorisation.	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have observed that Itadel has incorporated automatic access control, ensuring secure log-on to all relevant applications.	No significant exceptions noted.
9.4.3 Password management system *Password management systems should be interactive and should ensure quality passwords.* Itadel has drawn up guidelines on measures to ensure logical security, including logging and control of failed login attempts. These controls include: • Application requirements regarding use of passwords • Quality requirements regarding passwords • Requirements regarding lockout policy	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has drawn up guidelines on measures to ensure logical security that comply with the requirements of the Data Protection Agency. We have observed that the set-up includes: • Application requirements regarding use of passwords • Quality requirements regarding passwords • Requirements regarding lockout policy	No significant exceptions noted.

A.9 Control objective: Access control

Itadel's control activity	Control tests performed by PwC	Results of tests
• Log of and follow-up on failed login attempts • Control of failed login attempts • Requirements regarding password change at first login. Itadel has implemented controls in the systems ensuring that users are validated prior to a new password being allocated.	• Log of and follow-up on failed login attempts • Control of failed login attempts • Requirements regarding password change.	
9.4.4 Use of privileged utility programs *The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.* Itadel restricts access to systems and networks through two-factor authentication, and rights are managed through roles in Windows Active Directory. In addition, systems and data may only be accessed through the organisation's internal network; external access may only be obtained through a VPN connection.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that all rights, including access from other networks, are managed through roles in Windows Active Directory. We have observed that all access to data and systems is conditional on users having access the internal network, and, consequently, that external access may only be obtained through a VPN connection.	No significant exceptions noted.

A.11 Control objective: Physical and environmental security

Itadel's control activity	Control tests performed by PwC	Results of tests
11.1.1 Physical security perimeter *Security perimeters should be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.* Itadel has drawn up guidelines on physical security perimeters. Among other things, Itadel has established a security organisation responsible for enforcing physical security at Itadel's facilities. These controls include a number of access controls in facilities where personal data are being processed (admission cards and passwords). By entering into agreements with external parties, Itadel ensures that the external party is properly informed of IT security requirements.	We have briefly discussed the procedures/control activities performed with Management. We have observed that Itadel has drawn up guidelines on physical security, including that Itadel has established an IT security organisation. We have verified that Itadel has drawn up guidelines on physical security and that the physical access controls function as described. We have furthermore verified that Itadel has obtained an audit report from its subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	No significant exceptions noted.
11.1.2 Physical entry controls *Secure areas should be protected by appropriate entry controls to ensure that only authorised personnel are allowed access.* Itadel has drawn up guidelines on physical security	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has drawn up guidelines on physical security, including that Itadel has established an IT security organisation.	No significant exceptions noted.

A.11 Control objective: Physical and environmental security

Itadel's control activity	Control tests performed by PwC	Results of tests
perimeters. Among other things, Itadel has established a security organisation responsible for enforcing physical security at Itadel's facilities. These controls include a number of access controls in facilities where personal data are being processed (admission cards and passwords). By entering into agreements with external parties, Itadel ensures that the external party is properly informed of IT security requirements.	We have observed that Itadel has drawn up guidelines on physical security, and we have verified that physical access controls function as described. We have observed that Itadel has obtained an audit report from its subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	
11.1.3 Securing offices, rooms and facilities *Physical security for offices, rooms and facilities should be designed and applied.* Itadel has drawn up guidelines on physical security. These guidelines include a number of access controls in facilities where personal data are being processed (admission cards and passwords). By entering into agreements with external parties, Itadel ensures that the external party is properly informed of IT security requirements.	We have briefly discussed the procedures/control activities performed with Management. We have observed that Itadel has drawn up guidelines on the separation of facilities accessible to the public and internal office facilities. We have observed that the physical access controls function as described. We have furthermore verified that Itadel has obtained an audit report from its subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	During our audit of access lists for the selected data centres, we have observed that documentation for a single site could not be obtained. No further significant exceptions noted.
11.1.4 Protecting against external and environmental threats *Physical protection against natural disasters, malicious attack or accidents should be designed and applied.* Itadel has placed its data centres in buildings that are protected against natural disasters, malicious attacks and accidents.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that the data centres are located in buildings protected against natural disasters and malicious attacks. We have furthermore observed that the data centres are protected against lightning strikes and that this is subject to testing every five years. Through inspection, we have observed that IT systems are subject to these procedures and control activities.	No significant exceptions noted.
11.1.5 Working in secure areas *Procedures for working in secure areas should be designed and applied.* People without proper authorisation, who are granted access to Itadel's locations for specific business purposes, are received by the staff in the reception who handles registration and issues a visitor's pass. All guests are escorted by the employees with whom they have made an agreement.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that all guests visiting Itadel are provided with a visitor's pass and are escorted by an Itadel employee during the entire visit.	No significant exceptions noted.
11.2.1 Equipment siting and protection *Equipment should be sited and protected to reduce the risks*	We have briefly discussed the procedures/control activities performed with Management.	No significant exceptions noted.

A.11 Control objective: Physical and environmental security

Itadel's control activity	Control tests performed by PwC	Results of tests
from environmental threats and hazards, and opportunities for unauthorised access. Itadel's active data centres are protected against physical threats such as fire, water and heat. Fire protection, fire alarms and fire-fighting equipment as well as 24-hour manned monitoring of data centre infrastructure have been established.	By inspection, we have observed that Itadel has established guidelines on the protection against fire, water and heat. We have furthermore observed that Itadel has obtained an audit report from its subcontractor with a view to ensuring that similar requirements are met in areas subject to outsourcing.	
11.2.2 Supporting utilities *Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.* All infrastructure devices shared between active data centres are configured dimensionally with fully redundant systems, each with individual backup. Network connections from Itadel's active data centres are furthermore fully redundant.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established a fully redundant infrastructure with individual backup.	No significant exceptions noted.
11.2.3 Cabling security *Power and telecommunications cabling carrying data or supporting information services should be protected from interception, interference or damage.* Itadel's supply wires are secured underground and/or through casing. Wires are furthermore secured in operational facilities to which only authorised employees have access (by means of their tags and personal access codes).	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have furthermore investigated whether: • access to Itadel's locations is restricted to authorised employees, including through personal ID, as stated in the guidelines on securing offices and other facilities • wires critical to operations are underground or subject to adequate alternative protection.	No significant exceptions noted.
11.2.4 Equipment maintenance *Equipment should be correctly maintained to ensure its continued availability and integrity.* Itadel has entered into service agreements and introduced working schedules for equipment in data centres on call. The equipment in data centres is subject to inspection at least once a year.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has entered into agreements with external suppliers for the purpose of ensuring regular maintenance of protective equipment installed in data centres. We have moreover observed that service reports exist, documenting that maintenance of protective equipment has been performed within the last year. Through inspection, we have observed that IT systems are subject to these procedures and control activities.	During our audit of the procedures for maintenance of equipment in data centres, we have observed that there is no overall documentation method / procedure for storing all service reports for all data centres. We observed by sample testing that service reports for a number of devices could not be obtained. No further significant exceptions noted.
11.2.5 Removal of assets *Equipment, information or software should not be taken off-*	We have briefly discussed the procedures/control activities performed with Management.	No significant exceptions noted.

A.11 Control objective: Physical and environmental security

Itadel's control activity	Control tests performed by PwC	Results of tests
site without prior authorisation. Itadel has established guidelines ensuring that off-site removal of equipment, information and software is subject to authorisation being granted prior to removal.	By inspection, we have observed that Itadel has established guidelines ensuring that off-site removal of equipment, information or software is subject to authorisation being granted prior to removal.	
11.2.6 Security of equipment and assets off-premises *Security should be applied to off-site assets taking into account the different risks of working outside the organisation's premises.* Itadel has established guidelines on the use of assets off-premises.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established guidelines on the use of assets off-premises. We have furthermore observed that access to systems and data off-premises is protected through two-factor authentication.	No significant exceptions noted.
11.2.7 Secure disposal or re-use of equipment *All items of equipment containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.* Itadel has established guidelines on the disposal or re-use of equipment ensuring that information is not disclosed to unauthorised persons.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established guidelines on secure disposal or re-use of equipment. We have observed that Itadel has implemented relevant controls in relation to B4Restore's handling of backup. We have furthermore received an audit report from B4Restore and reviewed the requirements to be met by B4Restore in its capacity as subcontractor.	No significant exceptions noted.
11.2.8 Unattended user equipment *Users should ensure that unattended equipment has appropriate protection.* Itadel has established guidelines to ensure that equipment is not left unattended and, similarly, that equipment is suitably protected.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that guidelines have been established, ensuring that equipment is not left unattended. We have furthermore observed that an automatic screensaver is activated by the operating system following 10 minutes of inactivity.	No significant exceptions noted.

A.12 Control objective: Operations security

Itadel's control activity	Control tests performed by PwC	Results of tests
12.1.1 Documented operating procedures *Operating procedures should be documented and made available to all users who need them.* General and customer-tailored operating procedures have been documented in Itadel's internal operating portal, including intranet, shared drive and Configuration Management Database (CMDB).	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that operating procedures have been established through CMDB and that these are subject to updating at least once a year. We have furthermore observed that the operating procedures are accessible to all relevant employees.	During our audit of the operating procedures, we have observed that changes in customer operating systems are not consistently registered in a single system (CMDB or the like). We have been informed that all changes are recorded in different systems.

A.12 Control objective: Operations security

Itadel's control activity	Control tests performed by PwC	Results of tests
	By inspection, we have observed that IT systems are subject to these procedures and control activities.	No further significant exceptions noted.
12.1.2 Change management *Changes to the organisation, business processes, information processing facilities and systems that affect information security should be controlled.* Itadel has introduced formalised internal guidelines, procedures and descriptions. These include: • Incident management • Problem management • Change management • Release and patch management • User administration.	We have briefly discussed the procedures/control activities performed with Management. We have observed that Itadel has drawn up procedures for annual review and updating of: • Incident management • Problem management • Change management • Release and patch management • User administration.	No significant exceptions noted.
12.1.3 Capacity management *The use of resources should be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.* Itadel has drawn up procedures for monthly reporting on operations. These reports include information on production environment operations, including information on capacity. Automatic monitoring of the operating environment and relevant system parameters has been established, including of capacity, to ensure that future capacity requirements are met.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that reports on production environment operations at Itadel are sent to customers each month. We have furthermore observed that the capacity of production systems at Itadel is monitored to ensure that future capacity requirements are met.	No significant exceptions noted.
12.1.4 Separation of development, testing and operational environments *Development, testing, and operational environments should be separated to reduce the risks of unauthorised access or changes to the operational environment.* Itadel has established separate IT environments for development, testing and production. Only functionally segregated employees are able to migrate changes between the individual environments.	We have briefly discussed the procedures/control activities performed with Management. We have observed that in accordance with guidelines, Itadel has established separate environments for development, testing and operation and appropriate segregation of duties in connection with the operation of new functionality.	No significant exceptions noted.
12.2.1 Controls against malware *Detection, prevention and recovery controls to protect against malware should be implemented, combined with appropriate user awareness.*	We have briefly discussed the procedures/control activities performed with Management. By inspection of random samples, we have observed that employees' computers and servers at Itadel are protected by anti-virus software	No significant exceptions noted.

A.12 Control objective: Operations security

Itadel's control activity	Control tests performed by PwC	Results of tests
Itadel has established a procedure that protects systems and data against malicious data and programs. As a minimum, anti-virus software and/or anti-spyware systems are installed on machines and clients at Itadel; the software and/or systems are subject to regular updating.	– and that this software is up to date.	
12.3.1 Information backup *Backup copies of information, software and system images should be taken and tested regularly in accordance with an agreed backup policy.* Itadel performs backup of data at planned intervals. Backup data are tested continually through restore for the purpose of ensuring that data can be restored from backup. A process has been established to test whether backup and restore function as intended prior to implementing project sales solutions. Backup is monitored, making it possible to act timely on detected errors that may affect the operating services.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have investigated whether controls implemented function in accordance with guidelines: • whether backup is tested continually • whether monitoring has been implemented to ensure that continuous and correct backup is performed. A third party is responsible for the operation of the backup solution. We have observed that procedures and controls function in accordance with Itadel's security standards. We have tested that backup of systems is configured appropriately.	No significant exceptions noted.
12.4.2 Protection of log information *Logging facilities and log information should be protected against tampering and unauthorised access.* Itadel has established logging facilities, and these are protected against unauthorised access.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established logging facilities that are accessible only to employees whose job function justifies such access. We have observed that log information cannot be edited or deleted. Also, Itadel performs backup of the log information several times a day, and access is restricted to a few people.	No significant exceptions noted.
12.4.3 Administrator and operator logs *System administrator and system operator activities should be logged and the logs protected and regularly reviewed.* High-risk operating systems and network transactions or activities as well as the use of privileged rights are monitored. Deviations are examined and resolved in a timely manner.	We have briefly discussed the procedures/control activities performed with Management. Using random samples of technical set-ups, we have investigated whether: • logging of critical transactions and use of privileged access rights have been implemented • a process exists for timely follow-up on deviations. By inspection, we have observed that IT systems are subject to these procedures and control activities.	No significant exceptions noted.
12.4.4 Clock synchronisation *The clocks of all relevant information-processing systems*	We have briefly discussed the procedures/control activities performed with Management.	No significant exceptions noted.

A.12 Control objective: Operations security

Itadel's control activity	Control tests performed by PwC	Results of tests
within an organisation or security domain should be synchronised to a single reference time source. Itadel has synchronised all relevant information-processing systems to a single reference time source.	By inspection, we have observed that Itadel has established a reference time source for clock synchronisation of all relevant information-processing systems.	
12.5.1 Installation of software on operational systems *Procedures should be implemented to control the installation of software on operational systems.* Itadel ensures that changes to operating systems, databases, middleware and networks are tested/evaluated by qualified personnel before changes are made to operating systems. Tests of changes to operating systems, databases, middleware and networks must be approved before changes are made to operating systems. Changes to operating systems are made by qualified operations technicians. Emergency changes to operating systems, databases, middleware and network, which for operational reasons must be implemented outside the normal course of business, must be tested/evaluated and approved subsequently.	We have briefly discussed the procedures/control activities performed with Management. Using random samples from the system used for documenting changes, we have investigated whether – in accordance with guidelines – changes to the operating environment are carried out utilising a controlled process, including whether: • an approved test is performed prior to changes being implemented • testing and approval of emergency changes to the operating environment are documented immediately after being implemented.	During our audit of selected servers, we have observed a number of uncertainties regarding the definition of roles for Itadel and the customers in relation to the administrative rights and updates of some Windows and Unix servers. No further significant exceptions noted.
12.6.1 Management of technical vulnerabilities *Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.* Itadel has established monitoring systems that are configured to detect errors in the operating systems based on predefined criteria. System-generated errors are addressed and resolved in a timely manner.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that the operating systems are monitored and that they are configured to detect errors based on predefined criteria. We have furthermore observed that errors detected are examined and resolved in a timely manner. Regarding security updates of platforms and databases, we have observed that contractual agreements on planned service windows have been entered into.	No significant exceptions noted.
12.6.2 Restrictions on software installation *Rules governing the installation of software by users should be established and implemented.* Itadel has drawn up guidelines on the installation of software by users.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that guidelines concerning users' rights to download software have been drawn up. Using random samples, we have observed that the operating system has built-in restrictions to ensure that only approved applications may be installed/downloaded.	During our audit of client set-up, we have been informed that users have local administrative rights. We have been informed that Itadel is planning to remove local administrative rights from clients in 2019. No further significant exceptions noted.

A.13 Control objective: Communication security

Itadel's control activity	Control tests performed by PwC	Results of tests
13.1.1 Network security management *Networks should be managed and controlled to protect information in systems and applications.* Itadel controls network security through several control measures. Customers are provided with individual VLANs under which the customers' solutions are separated into a range of secure zones that are part of the security architecture. Guidelines have been established to ensure network traffic and connections between customer environments and the internet. For example, it is ensured that non-encrypted connections are not allowed, e.g. to the internal network from the internet. Editing of network infrastructure and customer environments is exclusively performed by authorised personnel verified by two-factor authentication and AD groups. Changes that cannot be considered standard changes are subject to the change management process. According to agreement, penetration tests are performed to ensure the security of customer networks.	We have briefly discussed the procedures/control activities performed with Management, and, through inspection of random samples, we have investigated whether – in accordance with guidelines – an appropriate security architecture has been established in the network, including whether: • the network is segregated into secure zones and whether customer environments are separated from Itadel's own environment • remote access is granted through two-factor authentication • changes to the network environment included in our sample have been made in a controlled manner in accordance with the change management rules.	No significant exceptions noted.
13.1.2 Security of network services *Security mechanisms, service levels and management requirements of all network services should be identified and included in network services agreements, whether these services are provided in-house or outsourced.* Itadel has established appropriate procedures for data communication to reduce the risk of loss of integrity, availability and confidentiality. Furthermore, the network has been segregated into a technical and administrative network as well as private networks pursuant to agreement with customers. Also, remote access via an external connection is managed through VPN using two-factor authentication.	We have briefly discussed the procedures/control activities performed with Management. We have reviewed the technical security architecture, and by inspection of random samples, we have investigated whether – in accordance with guidelines – an appropriate security level has been established, including whether: • the network is segregated into secure zones • data communication is managed through firewalls • remote access is granted through two-factor authentication.	No significant exceptions noted.
13.1.3 Segregation in networks *Groups of information services, users and information systems should be segregated on networks.* Itadel controls network security through several control	We have briefly discussed the procedures/control activities performed with Management. We have reviewed the technical security architecture, and by inspection of random samples, we have investigated whether – in	No significant exceptions noted.

A.13 Control objective: Communication security

Itadel's control activity	Control tests performed by PwC	Results of tests
measures. Customers are provided with individual VLANs under which the customers' solutions are separated into a range of secure zones that are part of the security architecture. All editing of network infrastructure and customer environments is exclusively performed by authorised personnel verified by two-factor authentication and AD groups.	accordance with guidelines – an appropriate security level has been established, including whether: • secure zones and customer environments are separated from Itadel's own environment • access to the network is segregated into relevant user groups based on users work related need • remote access is granted through two-factor authentication.	
13.2.3 Electronic messaging *Information involved in electronic messaging should be appropriately protected.* Itadel has established formalised procedures for the processing and destruction of input and output data material. These controls include: • Validation controls for input data material • Guidelines on secure destruction of output data.	We have briefly discussed the procedures/control activities performed with Management. We have verified that Itadel has implemented formalised procedures for the processing and destruction of input and output data material. We have verified that controls regarding validation of input data material and guidelines on secure destruction of output data material have been established.	No significant exceptions noted.

A.14 Control objective: Acquisition, development and maintenance of systems

Itadel's control activity	Control tests performed by PwC	Results of tests
14.1.1 Information security requirements analysis and specification *The information security-related requirements should be included in the requirements for new information systems or enhancements to existing information systems.* Itadel has drawn up procedures for information security management in connection with projects. The purpose is to ensure that projects (internal and external) and information systems meet relevant security requirements.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that Itadel has established a security organisation enforcing an appropriate level of information security in systems.	No significant exceptions noted.
14.2.4 Restrictions on changes to software packages *Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.* Itadel has imposed restrictions on access rights to modify software packages. On the machines, only a few accounts with administrative access are able to implement new software	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that access to operating systems is restricted. We have observed that only a few employees have rights enabling them to apply changes to software packages on machines. We have furthermore observed that these rights are assigned based on	No significant exceptions noted.

A.14 Control objective: Acquisition, development and maintenance of systems

Itadel's control activity	Control tests performed by PwC	Results of tests
packages.	employees' job function. By inspection, we have observed that IT systems are subject to these procedures and control activities.	
14.2.6 Secure development environment *Organisations should establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.* Itadel has established development, testing and operating environments that support the entire system development lifecycle.	We have briefly discussed the procedures/control activities performed with Management. By inspection of the machines at Itadel, we have observed that development, testing and operating environments have been established and that these are used in ISO and non-ISO environments, respectively. By inspection, we have observed that IT systems are subject to these procedures and control activities.	No significant exceptions noted.

A.15 Control objective: Supplier relationships

Itadel's control activity	Control tests performed by PwC	Results of tests
15.1.1 Information security policy for supplier relationships *Information security requirements for mitigating the risks associated with supplier's access to the organisation's assets should be agreed with the supplier and documented.* By entering into agreements with external parties, Itadel ensures that the external party is properly informed of IT security requirements, non-disclosure agreements, etc.	We have briefly discussed the procedures/control activities performed with Management. We have verified that agreements with subcontractors and B4Restore are signed and includes requirements regarding IT security.	No significant exceptions noted.
15.1.2 Addressing security within supplier agreements *All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organisation's information.* By entering into agreements with external parties, Itadel ensures that relevant security requirements are met by the individual supplier.	We have briefly discussed the procedures/control activities performed with Management. We have verified that agreements with subcontractors include requirements regarding IT security. We have verified that the subcontractor B4Restore provides Itadel with independent auditor's reports.	No significant exceptions noted.
15.1.3 Information and communication technology supply chain *Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and*	We have briefly discussed the procedures/control activities performed with Management. We have verified that agreements with subcontractors include requirements regarding IT security. We have verified that internal controls and procedures regarding	No significant exceptions noted.

A.15 Control objective: Supplier relationships

Itadel's control activity	Control tests performed by PwC	Results of tests
product supply chain. Procedures have been drawn up to ensure that agreements concluded with suppliers address relevant risks associated with the supply chain by enforcing risk management of the product and availability of services.	relevant risk assessments have been established.	
15.2.1 Monitoring and review of supplier services *Organisations should regularly monitor, review and audit supplier service delivery.* Itadel prepares monthly service reports for customers in which various matters pertaining to operations are documented and compared with applicable SLAs.	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that monthly service reports on the systems at Itadel are prepared. We have furthermore observed that these service reports include clear references to applicable SLAs.	No significant exceptions noted.

A.16 Control objective: Information security incident management

Itadel's control activity	Control tests performed by PwC	Results of tests
16.1.1 Responsibilities and procedures *Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.* The organisational responsibility for information security is documented and implemented at Itadel. Information security and related initiatives are handled by the operating organisation and supported by a dedicated security function, i.e. a staff function assisting the technical organisation.	We have briefly discussed information security governance with Management. We have verified that an appropriate security organisation supporting Itadel's business areas has been set up.	No significant exceptions noted.
16.1.2 Reporting information security events *Information security events should be reported through appropriate management channels as quickly as possible.* Itadel has implemented rules and procedures ensuring that information security incidents are reported.	We have briefly discussed the procedures/control activities performed with Management and by inspection investigated whether procedures for timely reporting of security incidents have been implemented. By inspection, we have observed that there is a formal procedure for reporting to customers.	During our audit of procedures for recording information-security incidents, we have observed that the process is manual. Consequently, there are no procedures that ensure that all events are recorded in a timely manner. No further significant exceptions noted.
16.1.3 Reporting information security weaknesses *Employees and contractors using the organisation's information systems and services should be required to note and report any observed or suspected information security*	We have briefly discussed the procedures/control activities performed with Management. By inspection, we have observed that incidents registered are reported by all relevant parties.	No significant exceptions noted.

A.16 Control objective: Information security incident management

Itadel's control activity	Control tests performed by PwC	Results of tests
weaknesses in systems or services. Itadel has established guidelines to ensure that any suspected security weaknesses in systems and services are recorded and reported to customers pursuant to agreement.		
16.1.4 Assessment of and decision on information security events *Management responsibilities and procedures should be established to ensure a quick, effective and orderly response to information security incidents.* The organisational responsibility for information security is documented and implemented at Itadel. Information security and related initiatives are handled by the operating organisation and supported by a dedicated security function, i.e. a staff function assisting the technical organisation.	We have briefly discussed information security governance with Management. We have verified that an appropriate security organisation supporting Itadel's business areas has been set up.	No significant exceptions noted.
16.1.5 Response to information security incidents *Information security incidents should be responded to in accordance with the documented procedures.* Itadel has implemented rules and procedures ensuring that information security incidents are reported.	We have briefly discussed the procedures/control activities performed with Management and by inspection investigated whether procedures for timely reporting of security incidents have been implemented.	No significant exceptions noted.

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

Itadel's control activity	Control tests performed by PwC	Results of tests
17.1.1 Planning information security continuity *The organisation should determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.* Itadel has taken the necessary measures and implemented contingency plans with a view to ensuring the recovery of operating systems in a crisis/disaster. The contingency plan details the establishment of a contingency organisation, including rooms and access, guidelines to be followed by the contingency management team, staffing, lists of systems, recovery/business continuity operations, instructions regarding activities and communication, contact lists, etc.	We have briefly discussed the procedures/control activities carried out with Management. By inspection, we have furthermore investigated whether – in accordance with guidelines – a suitable contingency plan for operations has been drawn up.	No significant exceptions noted.

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

Itadel's control activity	Control tests performed by PwC	Results of tests
17.1.2 Implementing information security continuity *The organisation should establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.* Itadel has taken the necessary measures and established contingency plans for recovery of operating systems during an adverse situation. The contingency plan details the establishment of a contingency organisation, including rooms and access, guidelines to be followed by the contingency management team, staffing, lists of systems, recovery/business continuity operations, instructions regarding activities and communication, contact lists, etc.	We have briefly discussed the procedures/control activities carried out with Management. By inspection, we have furthermore investigated whether – in accordance with guidelines – a suitable contingency plan for operations has been drawn up.	No significant exceptions noted.
17.1.3 Verify, review and evaluate information security continuity *The organisation should verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.* Itadel has established procedures to ensure that the contingency plan is reviewed once a year and tested through high-impact operational disturbances, such as breakdown of the central data-centre infrastructure.	We have briefly discussed the procedures/control activities carried out with Management. By inspection, we have investigated whether – in accordance with guidelines – the contingency plan is tested at regular intervals, whether issues identified are documented and whether remedial measures are incorporated in the contingency plan.	No significant exceptions noted.

A.18 Control objective: Compliance

Itadel's control activity	Control tests performed by PwC	Results of tests
18.1.1 Identification of applicable legislation and contractual requirements *All relevant legislative statutory, regulatory, contractual requirements and the organisation's approach to meet these requirements should be explicitly identified, documented and kept up to date for each information system and the organisation.* Itadel has drawn up procedures to ensure compliance with applicable legislation and contractual requirements.	We have briefly discussed the procedures/control activities performed with Management. We have verified that Itadel enters into agreements concerning the specific control activities carried out at Itadel in relation to the SLAs.	No significant exceptions noted.