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.

Unit IT A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2021 to 31 December 2021 in relation to Unit IT A/S' operational services and hosting activities to customers

January 2022

Contents

1 Management's statement

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

Unit IT A/S uses FrontSafe A/S as a subservice supplier for backup storage. This report uses the carve-out method and does not comprise controls that FrontSafe A/S performs for Unit IT A/S.

Unit IT A/S confirms that:

a) The accompanying description in section 2 fairly presents Unit IT A/S' operational services and hosting activities that have handled customers' transactions throughout the period from 1 January 2021 to 31 December 2021. The criteria used in making this statement were that the accompanying description:

(i) Presents how IT general controls in relation to Unit IT A/S' operational services and hosting activities were designed and implemented, including:

- The types of services provided

- The procedures, within both information technology and manual systems, by which the IT general controls were managed

- Relevant control objectives and controls designed to achieve those objectives

- Controls that we assumed, in the design of Unit IT A/S' operational services and hosting activities, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description

- How the system dealt with significant events and conditions other than transactions

- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to IT general controls.

(ii) Includes relevant details of changes to IT general controls in relation to Unit IT A/S' operational services and hosting activities during the period from 1 January 2021 to 31 December 2021

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2021 to 31 December 2021. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2021 to 31 December 2021.

Middelfart, 7 January 2022

Mark Frihagen, CEO

2 *Unit IT A/S' description of IT general controls in relation to operational services in Denmark*

Summary – Unit IT A/S in short

The company stems from the **world-wide** USTC corporation in Middelfart and was until 2003 an internal IT department for the many companies within the corporation, among others, shipowners, ship transport and bunker oil.

Unit IT was forged from three highly skilled IT vendors, each covering their specialty. You used to know us as Outforce, Mindzet and it-Craft. In 2018, we adopted our new uniform brand to display that we are now one company with a wide range of services.

Unit IT A/S provides consulting for, designs, services, implements and operates IT solution, focusing on:

- We deliver dedicated, hosted IT solutions with 24/7 operations
- We deliver IT infrastructure projects
- We are quality minded, and always deliver according to established best practices
- We deliver on time
- We are easy to partner with and maintain a "Keep It Simple" approach.

Description of services

Unit IT A/S' primary services are as follows:

- Provision of private cloud services including the Windows operating system
- High performance storage solutions
- Customer-specific Remote Desktop and Citrix solutions
- MS Exchange and Office365
- Helpdesk and client support
- SQL as a service
- Image and remote backup.

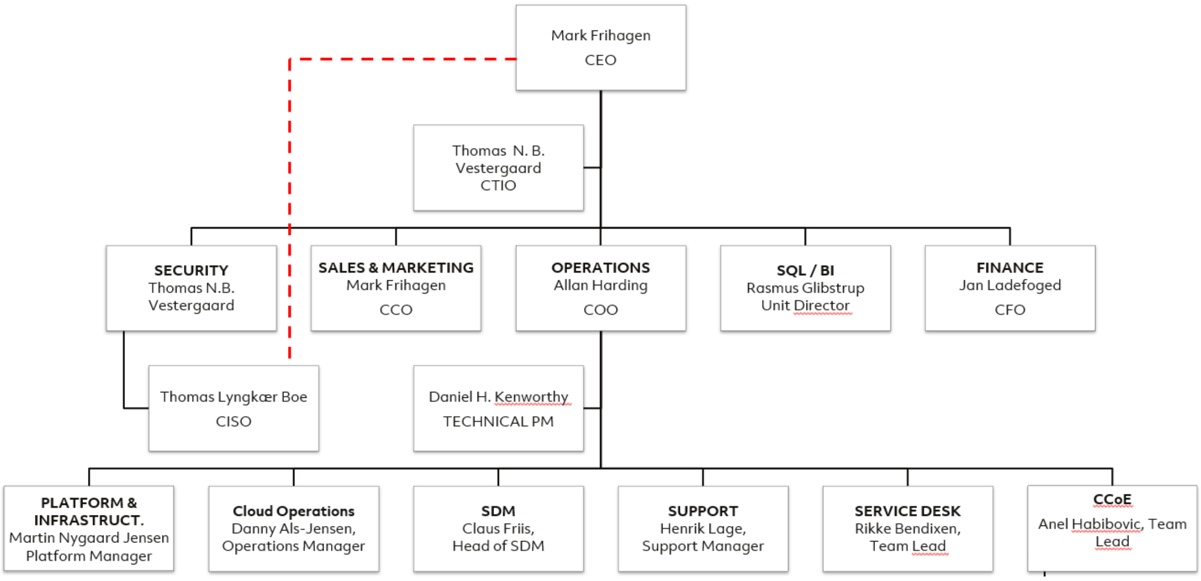
Unit IT A/S currently has 2 data centres of its own in Middelfart and a co-location in Kolding, with approx. 24 km between the 2 data centres and the co-location. From here, approx. 2,500 servers are monitored and operated.

Unit IT A/S' support team runs two shifts, so they are physically manned from 6:00 – 21:00. All employees can provide support in Danish and English, with a few also able to do so in German. Unit IT A/S provides first level user support to more than 5,000 users.

This description encompasses operations and monitoring from 1 January 2021 – 31 December 2021 and is exclusively for the use of the companies that use Unit IT A/S' IT operations and hosting activities and the auditors of these companies and may not be used for other purposes.

Risk management

Organisational structure of Unit IT A/S



Management has the overall responsibility for Unit IT A/S' security work.

Unit IT A/S' guiding principle is that information security is based on the real risks that Unit IT A/S is exposed to. Therefore, with ISO 27005 as a framework tool, we assess the risk management as described below.

Established conditions in risk management are assessed geographically, in terms of IT and politically based on a qualitative impact and probability assessment, and, respecting the changing world around Unit IT A/S, Unit IT A/S will continuously assess the need for adjusting the company's risk management.

	Preventative measures	**Remedial measures**
Administrative measures	Policies and guidelines Awareness Change management CAB board Technical management Compliance controls Supplier contracts Service and support agreements System documentation	Emergency plans Logging Disaster recovery procedures Procedure for major incidents
Physical and technical measures	Firewalls Antivirus Alarm systems Test environments Monitoring Intrusion prevention Redundancy User management Clusters Password policy	Standby equipment Backup/restore Virtualisation Standby site Server snapshots Intrusion detection Fire extinguishing Standby power

Unit IT A/S makes continual use of external partners like Arrow ECS, Lenovo and HP to ensure that our installation is constructed and maintained according to best practice in relation to technology and security.

It is up to the customer to demand specific safety practices or technical installations, if Unit IT A/S' standard does not live up to best practice in relation to technology and security.

Control environment

Unit IT A/S has chosen to use the ISO 27000 series as a framework for establishing the control environment, which means that components from the ISO 27000 series have been reviewed and evaluated in relation to implementation in the company. Unit IT A/S considers ISO 27000 to be an essential safety standard in efforts to build and address a compliant and consistent approach to the control environment and IT security policies in Unit IT A/S.

Our methodology for the implementation of controls s defined with reference to ISO 27002 (set of rules for controlling information security), and Unit IT A/S has worked with the following control and safety measures:

- General guidelines
- Organisation of information security
- Management of information related assets
- Employee security
- Physical security
- Network management and operation
- Access control
- Acquisition, development and maintenance of information processing system
- Management of security incidents
- Emergency management
- Compliance with statutory and contractual requirements.

Unit IT A/S is divided into functional business units (see the organisational plan in the Risk management section) and thus has the ability to work in a structured manner with the guiding and normative requirements in the ISO 27000 series. In addition, the structural composition provides good conditions for providing and maintaining a high level of service to Unit IT A/S customers. Unit IT A/S considers a high level of service and high customer satisfaction to be essential in minimising risks for Unit IT A/S.

Unit IT A/S is headed by Managing Director Mark Frihagen, who reports to the USTC group. Unit IT A/S currently has approximately 100 employees.

The operations organisation currently has approximately 50 employees and comprises the following teams:

- Managed Services. The primary function of this team is to ensure stable operation and maximum uptime, as well as to handle scheduled service windows on the data centre infrastructure.

- Platform & Infrastructure. Manages the monitoring of servers, networks, storage and WAN connections, including VPNs and layer 2 connections to customers. In addition, the team manages the installation and customisation of Windows OS, Exchange and Citrix.

  The team is responsible for the implementation of new customers, including scheduling.

  The team also has external tasks with onsite customers outside the data centres. License reporting is also handled by the team.

- Support. The primary function of this team is to provide user support for the hosted solutions, including support of PCs and MAC, as well as addressing general customer questions.

  The Support team operates on a two-shift basis and is thus physically manned from 6 a.m. to 9 p.m. All employees offer support in Danish and English. Unit IT A/S provides first level user support to more than 5,000 users.

- Service Desk is the contact point between customers and our employees. The purpose is to ensure that the customer is always met with appropriate and timely help for all types of enquiries.

Service Desk checks and coordinates enquiries regarding e.g. IT breakdowns, requests for new assignments, changes to customer's IT environment and minor projects.

In brief, Service Desk is responsible for ensuring that the right experts and specialists solve exactly the assigned task within the agreed deadline and financial framework.

Service Desk is designed to handle the flow for incidents (e.g. IT breakdowns), Service Requests (request or new assignment) and Change Requests (change in IT environment) and handles Vendor Management.

The Service Desk phone line is open 24/7 for enquiries regarding critical incidents that require immediate assistance.

- Service Delivery Management ensures that services agreed in the contract are delivered in due time and at the agreed quality.

  Service Delivery Management handles all reporting of operational services as well as KPI and SLA metrics. Furthermore, the team holds operating status and steering group meetings with customer and supplier representatives.

  Service Delivery Management is also the escalation point in case of disputes and acts as Situation Manager 24/7 in case of critical incidents.

  If requested by the customer, Service Delivery Management acts as a trusted advisor to the customer and as a coordinator between the customer and third-party suppliers.

In addition, organisations exist for handling Sales & Marketing, SQL/BI, Finance and Innovation (see organisational chart above).

Organisation of information security

Unit IT A/S has, with ISO 27001 as a benchmark, qualitatively assessed the security measures and control procedures that Unit IT A/S is taking or is intending to take. We are aware in this context that this important work is a dynamic process and are taking this into account in the company's daily activities as well as in the existing and future strategy work.

Unit IT A/S has strategically chosen to offer customers high uptime as well as high and local accessibility, which requires a continuous focus on factors that maintain and improve reliability in Unit IT A/S.

Unit IT A/S is focused on a small, but significant number of customers (under 150) and has clearly formulated to be more for these large customers in an existing 3-year strategy.

Unit IT A/S has formulated goals and actions in the current strategy, which aims to address external factors that could pose a risk to information security.

Internally, we have formulated an Information Security Policy, which is rooted in the company's Personnel Handbook. The Personnel Handbook is easily accessible to all employees on the company's intranet, and all employees are given access to the terms and conditions when employed by Unit IT A/S.

Unit IT A/S uses a central log system with higher-level security functionality and external threat information to collect logs from key administrative systems in order to detect abnormal activity later.

At Unit IT A/S, the internal administrative security function is carried out by the CISO. The responsibility for the technical security is located in Operations. This function ensures the implementation and updating of security and quality procedures, is responsible for the primary contact with accountants/auditors, ensures the performance of self-checks, ensures the ongoing maintenance of risk assessment and ensures that there is a contingency plan (=the document "General business and operating procedures") and that it is regularly updated.

It is up to the individual employee keep abreast of the professional developments within their area and to keep their education level up to date. The employee is entitled to and required to take relevant further education, which is arranged with the immediate superior. Unit IT A/S will bear all costs for this education. Twice a year, MUS interviews about education are held – for some employees, a plan is made for a year at a time. This is stated in the minutes of the MUS interviews, where other personal matters are also described.

Unit IT A/S' general policies and procedures are described in the document "General business and operating procedures".

The responsibility for security policy, contingency plans, operating procedures and the description of business procedures lies with Management. It is Management who communicates externally with, for example, the press. Responsibility for the dissemination of business practices and internal routines lies with Management. Concerning updates/corrections, it is the responsibility of Management to convey these and anchor them.

Management of information-related assets

We have contracts for agreed services for all our customers. Specific circumstances are described herein as they were when the contract was entered into. Changes thereto are described in the appendix to the contract and they are implemented in Unit IT A/S' administrative systems with the attachment of the customer's approval.

Employee security

The Management of Unit IT A/S will ensure that all employees are familiar with their roles and responsibilities and that all are qualified and able to perform their role.

All employees must live up to the role assigned to them and follow our procedures. This is to ensure that, among other things, security-related issues are escalated and handled in order to take particular care of our customers' data and equipment and thus our reason for existence.

We have a procedure and a checklist for recruiting employees and establishing cooperation with managers, where we ensure that we hire the right candidate in terms of background and competence.

General terms of employment, including confidentiality about their own relationships and those of the customers, are described in each employee's employment contract, where conditions about all aspects of employment, including termination, are specified.

Physical security

External access control

All visitors must be entered into the logbook found at the reception. In addition to this, all visitors must carry visible guest cards.

Access control to data centres

Unit IT A/S has two operating centres which, besides being protected by a normal in-house alarm system, also have an additional alarm system that only covers the operating centres. A 4-digit code must be entered to switch the alarm system on and off. The code is personal for the individual employee and Operations handles and maintains these.

In addition to a code, a 3D facial scanner is used to control entry to data centre 1 and data centre 2. That is to say, both centres have physical access control in addition to a code.

Both data centres can be accessed by authorised personnel 24/7-365. Both data centres are monitored by video, and so are both cooling systems.

The data centre in Kolding is controlled by Global Connect, and Unit IT A/S' employees have access cards for the data centre in Kolding. If the card has not been used for 3 months, it will automatically be locked and will need to be reactivated.

Network management and operation

Overall description of the data centres

The primary data operation takes place in Unit IT A/S' data centre 1 and data centre 2. Data centres 1 and 2 are located on the same property, but are two separate data centres with redundant data lines from TDC, among others, and each has its own infrastructure, cooling, emergency power generator, UPS etc.

The data centres are connected to several fibre optic connections and operate independently, so that customers' IT installations are distributed across both data centres, reducing the risk of downtime. We use data centre 3 in Kolding for disaster recovery.

The building that houses data centre 1 and data centre 2 is protected by external video surveillance and access control on doors.

Only specially authorised personnel with an operational need for access are granted access to data centre 1 and data centre 2. In both data centres, access card and a unique code must be used to pass the control gate. At the control gate, a 3D facial scanner is used in combination with an access card to access the data centre.

Description of data centre 1:

- UPS emergency power with battery backup
- Emergency generators
- Fire protection with sprinklers
- Cooling plant
- Physical access control using a 3D facial scanner
- 24-hour monitoring of the server room connected to Dankontrol's alarm centre with alarms for humidity, temperature, fire, UPS and emergency power generator
- Physical spare parts stock
- Video surveillance.

Description of data centre 2:

- UPS emergency power with battery backup
- Emergency generator
- Fire protection with sprinklers
- Cooling plant
- Physical access control using a 3D facial scanner
- 24-hour monitoring of the server room connected to Dankontrol's alarm centre with alarms for humidity, temperature, fire, ups and emergency power generators
- Physical spare parts stock
- Video surveillance.

Backup and disaster recovery

Unless otherwise agreed, Unit IT performs data backup of all servers. The customer can opt out of this and instead supply its own backup solution. In addition, for virtual servers, a disaster recovery backup is made by default. The customer can opt out of this, too.

Unit IT A/S' ability to restore an IT environment relies on both data backup and disaster recovery backup.

Disaster recovery backup

Disaster recovery backup is used to re-establish virtual servers very quickly in any data centre. Data can be restored in both our data centres or alternatively in data centre 3, which is located in Kolding, 27 km from Unit IT A/S' data centres 1 and 2. All the data centres are connected with 10Gbit fibre for highest speeds.

Veeam Backup & Replication is used to perform disaster recovery (DR), and data is stored in data centre 3 in Kolding.

Generally, a DR backup of the C drive of all virtual servers is performed once a day with a 7-day history unless otherwise agreed with the customer.

Unit IT performs quarterly restore tests on the DR platform to check the functionality of the backup system in relation to restoring data. These restore tests only validate the system's ability to restore data and cannot replace the end customer's need for test and validation of data restore from backup.

Unit IT encourages all customers to regularly validate the integrity of their backup data.

Every day, Unit IT checks that all defined DR backups have been performed as planned. In the event of an error, the error is recorded, and corrective action is taken to secure a valid backup. Any deviations regarding unwanted DR backup are kept in the customer's CMDB on the server in question.

By default, new virtual servers are included in the DR backup. Unit IT carries out weekly checks to ensure that no virtual servers without DR backup exist unless the customer has explicitly opted this out.

Data backup

IBM Spectrum Protect technology (formerly known as TSM or Tivoli Storage Manager) is used for data backup. Backup data is located in 2 separate data centres 98 km away from Unit IT A/S' operating centre at Front-Safe in Aarhus. We have specialists at all levels and in all areas with interdisciplinary skills in the technologies used.

All servers, both physical and virtual, use this backup. Generally, data is encrypted with an encryption key chosen by the customer. This ensures that the stored backup data is unreadable to anyone but the customer. The customer owns the encryption key for backup data but makes it available to Unit IT to the extent necessary to operate the backup. File and database agents are used. Database agents for SQL, for example, can ensure that hourly backup of SQL data can be taken, if desired.

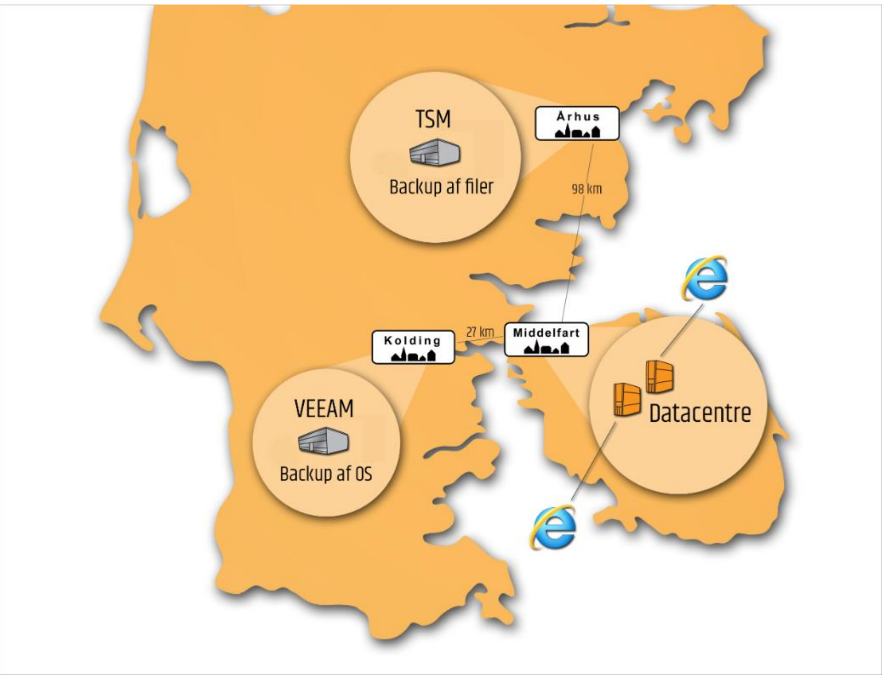
Incremental backup of all data is performed at least once a day unless otherwise agreed with the customer. In a standard data backup, data is sent directly to Front-Safe's IBM Spectrum Protect backup servers and storage. Subsequently, the customer's data is copied to Front-Safe's secondary data store, which has a different physical location. With a cloud backup solution, the customer has two offsite copies of its data.

In order to meet the high demands on performance, restore times or data reduction, the customer can opt for a hybrid backup solution instead of the standard data backup. With the hybrid solution, the customer has a local copy as well as an offsite copy of its backup data. The customer has a local IBM Spectrum Protect server, which is a front server. This front server synchronises its backup storage with the data store on Front-Safe's backup servers.

Every day, Unit IT checks that all defined data backups have been performed as planned. In the event of an error, the error is recorded, and corrective action is taken to secure a valid backup.

Unit IT carries out weekly checks to ensure that no servers without data backup exist unless the customer has explicitly opted this out. Any deviations regarding unwanted data backup are kept in the customer's CMDB on the server in question.

Principle diagram, backup and disaster recovery



Maintenance of systems

Patch management strategy

Updates are installed in the categories Security Updates, Critical Updates and Optional Updates. This allows patches to be classified according to relevance and importance for every customer. Unit IT A/S offers monthly patching of all versions of Windows Server that are under active maintenance from Microsoft. The frequency of updating is defined based on the individual customer's requirements for the availability of the solution (patch tag).

The customer also has the option of choosing automatic patching of standard applications such as internet browsers, Adobe Reader and Adobe Flash if these are installed on the customer's solution. To protect against known vulnerabilities in these standard applications, Unit IT A/S' customers are advised to take advantage of this.

Unit IT A/S regularly validates that operating systems as well as applications are installed correctly in the latest available version.

Change management strategy

Unit IT A/S' strategy in this area ensures that changes in existing user systems and operating environments follow formalised business practices and processes. This happens through these means:

- Registration and description of change requests
- All changes are subject to approval before formal implementation
- Changes are subject to formal impact assessments
- Fall-back plans are described where possible
- There is an identification of systems affected by changes
- There is a documented test of changes before implementation where possible
- Documentation is updated so that it essentially reflects the changes that have been made
- Procedures are governed and coordinated in Unit IT A/S' ITSM system.

Changes are evaluated in two ways, based on an assessment of impact and probability. Thus, a real classification of changes is made. However, a change form is always drawn up.

If this change form is LOW in impact, probability and classifications, it can be carried out without approval, by the individual technicians. Changes that have another classification than described must be approved by a manager in Operations. Unit IT A/S' SDM function ensures the correct filling out of change forms according to requirements before they are submitted for approval.

Access control

Access to IT systems

The logical security includes logical protection of electronic systems and information relating to providing the service. For example, it states that only authorised persons have access to it.

Unit IT A/S' strategy in this area ensures that employees are provided with adequate work tools and that these tools are continuously secured as security measures are taken. Unit IT A/S wants to be a flexible and attractive workplace, which is why the ability to connect remotely is offered for our own as well as our customers' IT systems. In order to secure these, the following elements are considered.

Access options

Access to Unit IT's administrative network and administrative systems is only available for authorised persons and requires two-factor validation. Authorisation can be provided via a combination of username/password and a one-time passcode (OTP) or via a combination of username/password and an approved computer authorised through a unique certificate (802.11x).

Operational systems can only be accessed via an additional access control, which is also subject to two-factor validation. Secondary usernames and passwords are used for accessing operational systems, and the same applies to all access to customer systems.

All communication with administrative systems, operational systems and customer systems that does not take place at a Unit IT location is encrypted.

Unit IT A/S has authorised mobile devices (smartphones, tablets mv.) to synchronise e-mails and calendars. Access to this data is controlled by an AD set-up. All devices that are synchronised are locked with a code after 15 minutes and it is not possible to change for individual employees.

Unit IT A/S' password policy requires at least 12 characters, including both numbers, letters and special characters. For standard users, the password must be changed every 60 days. Access to customer systems is given based on work-related needs and is managed through an administrator account for the individual employee. The password policy is the same as on a standard user. If an external person needs to login, he or she is created with a user and temporary access which is closed after the task is completed.

In order to avoid unintended access, employees must lock or log off their personal computers when leaving the workplace.

Dankontrol monitors both data centres electronically. That is, they look to see whether the alarm is connected at 20:30 at the latest. If it is not, the guard is called, thus ensuring the alarm is connected.

Acquisition, development and maintenance of information processing systems

Unit IT A/S will ensure that all new acquisitions and implementation of servers, systems, services and software are handled in a structured and secure manner.

We have a procedure for tasks of a certain size that can mean significant changes in our overall operating system for all customers or implementation of customer solutions, either they are handled through change management or our project manager (project management model).

Our project management model is based on our own and practical methodology but is divided into a series of phases: pre-analysis, design, testing, implementation, testing and evaluation. Each phase includes acceptance from stakeholders.

Management of security incidents

Unit IT A/S works with IT security at a business-strategic and risk-based level through its IT Security Committee. The IT Security Committee is represented by top management, CEO, CFO, COO and CISO, and the committee reports directly to the board of directors. The committee addresses material IT security issues, and the IT security is effected through policies, procedures and guidelines. Unit IT's CISO reports directly to the CEO and reports on Unit IT's threat level.

Unit IT A/S is a member of NC3Skyt at the Danish Centre for Cyber Security (Center for Cybersikkerhed) (NC3) under the Danish Defence Intelligence Service (Forsvarets Efterretningstjeneste) and also receives weekly threat information from the European Cybercrime Centre (*EC3*).

Our employees are included in the security rotation so that we can respond 24 hours a day. If an incident occurs outside normal working hours, it is the on-duty employee who assesses what reaction is needed. Then it is necessary to inform customers and the outside world. This is done by involving the Situation Management rota, constituted by SDMs.

If an incident occurs within normal working hours, employees will handle and escalate the case in the same way as other cases and with the priority required.

It is the employees' responsibility to report security breaches or suspicions of them to Management immediately. Likewise, the company's monitoring system will be set up to identify selected security breaches.

We keep up-to-date with identified weaknesses in the systems we use and offer via manufacturer support sites and discussion forums.

Through our membership of Danish Cloud Community (=DCC), we are committed to ensuring that critical security updates are implemented within two months of release. We ensure this by weighing and implementing all significant updates within the timeframe.

Emergency management

Information and communication

It is the responsibility of each team leader to communicate internally in Unit IT A/S. Management is responsible for communication to customers and the press. Reporting is prepared by the individual units and approved by Management before it is sent to the customer.

The manner in which things should be communicated is reflected in Unit IT A/S' Guide for Handling Major Incidents, which includes telephone contact, SMS communications and e-mails in a structured communication platform used by Unit IT A/S. Also defined in the procedure is who in Unit IT A/S communicates what, how and to whom. The procedure is defined in terms of roles and not individuals in Unit IT A/S.

Contingency plans

Identification of critical processes

The effort to elaborate business emergency plans has been identified and the work will be prepared in accordance with the identified needs. The overall management of Unit IT A/S will handle these in conjunction with the technical contingency plans.

Communication in the situation

One of the key elements for successful management of a preparedness situation is to ensure adequate communication to all relevant stakeholders in a timely manner and with the right content. Communications must ensure that the organisation's stakeholders are informed so well about the situation that confusion is minimised as much as possible.

Unit IT A/S has identified a preferred form of communication and roles, distributed in a framework, for dealing with Major Incidents. The responsibility for maintaining this process and role distribution rests with Management in Unit IT A/S. The procedure for handling Major Incidents is available to all employees on the company's intranet and is also available in hard copy in the company.

The effective communication is expected to prevent an unnecessary number of inquiries about the incident and unnecessary use of time and effort in order to handle the actual situation. Communications must also ensure that stakeholders get the necessary information to minimise any consequences and to establish any alternative solutions.

Communication preparedness, like technical preparedness, must be tested, which happens when an incident occurs – the process is also reviewed qualitatively on regular basis.

Unit IT A/S considers the minimum requirements for hosting as essential and Unit IT A/S uses procedures to ensure that Unit IT A/S always meets the applicable requirements for good hosting that the association of IT Hosting Companies in Denmark may require.

Technical preparedness

Unit IT A/S' technical contingency plans are summarised in the procedure description dealing with General Procedures and Operating Procedures 1.17, which includes FrozenZone, emergency power and testing, backup, firefighting, Denial-of-Service, creation and deletion of employees.

Control activities

Unit IT A/S only uses standard systems. The Disaster Plan is available on the intranet. In addition, there is a copy in data centre 3. The details appear from control objectives and control activities, according to a table with lists and tests.

Compliance with statutory and contractual requirements

We bring in an external auditor annually for the purpose of issuing a statement of compliance with the checks mentioned in this description. Because we are members of Danish Cloud Community, we must annually certify that we are complying with the ISAE 3402 framework. Said auditor's statement ensures, as the Danish Cloud Community requires, that the external auditor confirms our compliance with the association's other requirements relating to insurance matters, transparency in business conditions, corporate matters in our company, etc. These confirmations by the auditor help with Danish Cloud Community certification of our company.

Complementary user entity controls

As part of the delivery of services, the customer must implement certain controls that are important to achieve the control objectives specified in the description. These include:

- Consider/test new versions of systems at the implementation stage
- Handle the set-up and administration of own users in the production environment
- Handle the set-up and administration of users from Unit IT and external suppliers who provide assistance in the customer's environment
- Ensure that necessary data are included in support cases
- Inform Unit IT about changes in employees who have access to sites shared between the customer and Unit IT.

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

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2021 to 31 December 2021 in relation to Unit IT A/S' operational services and hosting activities to customers

To: Unit IT A/S and customers of Unit IT A/S' operational services and hosting activities and their auditors.

Scope

We have been engaged to provide assurance about Unit IT's description in section 2 of its IT general controls in relation to Unit IT's operational services and hosting activities which has processed customers' transactions throughout the period 1 January 2021 to 31 December 2021 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Unit IT A/S uses FrontSafe A/S as a subservice supplier for applied backup storage. This report uses the carve-out method and does not comprise controls that FrontSafe A/S performs for Unit IT A/S.

Unit IT's responsibilities

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

Service auditor's independence and quality control

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

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

Service auditor's responsibilities

Our responsibility is to express an opinion on Unit IT's description and on the design and operating effectiveness of controls related to the control objectives stated in that description, based on our procedures.

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

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of Unit IT's operational services and hosting activities 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 appropriately designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by Unit IT in the Management's statement section.

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

Limitations of controls at a service organisation

Unit IT'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 operational services and hosting activities that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions. Furthermore, the projection of any evaluation of effectiveness to future periods is subject to the risk that controls at a service organisation may become inadequate or fail.

Opinion

Our opinion has been formed on the basis of the matters outlined in this auditor's report. The criteria we used in forming our opinion are those described in the Management's statement section. In our opinion, in all material respects:

(a) The description fairly presents how IT general controls in relation to Unit IT's operational services and hosting activities were designed and implemented throughout the period from 1 January 2021 to 31 December 2021;

(b) The controls related to the control objectives stated in the description were appropriately designed throughout the period from 1 January 2021 to 31 December 2021; and

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2021 to 31 December 2021.

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

Aarhus, 7 January 2022
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper P. M

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Iraj Bastar
Director

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

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

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

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

4.2 Test actions

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

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

4.3 Control objectives, control activity, tests and test results

Control Objective A: Information security policy

Management has developed an information security policy that sets a clear goal for IT security, including the choice of frame of reference and allocation of resources. The information security policy is maintained by taking into account a current risk assessment.

Control objectives/control	PwC test	Result of test
Written policy for information security Unit IT A/S has developed a security policy. This is available to employees on the intranet. It is revised at least once a year and approved by Management.	We have made inquiries of Management about the procedures/control activities performed. We have inspected that Management has approved the security policy and that it is reviewed at least once a year. Furthermore, we have confirmed that it is readily available to employees.	No exceptions noted.

Control Objective B: Organisation of information security

The organisational responsibility for informational security is adequately documented and implemented, and the handling of external parties ensures and adequate treatment of security in agreements.

Control objectives/control	PwC test	Result of test
Management's responsibility in regard to information security The individual department managers are responsible for making new employees aware of the guidelines as part of their introduction to the company. When guidelines are updated, employees will be informed by e-mail and through the USTC network where the updated and current version of the security policy is also available.	We have made inquiries of Management about the overall control of information security. We have verified that the organisational responsibility for information security has been documented and implemented. In addition, we have made inspections of the reporting on information security incidents, and an inventory of assets has been prepared.	No exceptions noted.
External parties Unit IT A/S asks partners and external providers to send an auditor's statement regarding the agreed services or sign a contract setting out confidentiality and security measures. Unit IT A/S ensures that external partners are familiar with Unit IT A/S' security policy.	We have made inquiries of Management about the procedures/control activities performed. We have verified that adequate procedures for cooperation with external suppliers have been established. Using random samples, we have verified that cooperation with external parties is based on approved contracts and an auditor's statement has been received from backup providers for the relevant period.	No exceptions noted.

Control Objective C: Physical security

Operational management is carried out in premises that are protected from damage caused by physical conditions such as fire, water damage, power failure, theft or vandalism

Control objectives/control	PwC test	Result of test
Physical security controls All employees at Unit IT A/S have access to the premises through alarm systems. The offices lock automatically at 4:30 p.m. and open again at 7:30 a.m. Outside opening hours, employees must use a code and a tag to access the building. Access to the data centres is regulated by a code at the door to the workshop, and a 3D facial scanner controls entry to the data centres. Access to the data centres is given according to work needs. The data centres are video monitored. Unit IT A/S can thus document activities in the data centres. Guests are accompanied by an employee with access to the data centres.	We have made inquiries of Management about the procedures/control activities that are being carried out. We have observed that access to the data centres at Unit IT is restricted to employees with a work-related need. Using random samples, we have investigated procedures for physical access to secure areas to assess whether such access is subject to documented managerial approval and whether individuals without authorisation to secure areas must register and must be escorted by an employee with the proper authorisation.	No exceptions noted.
Securing of offices, premises and facilities Data centres are access-controlled with a code on the door of the workshop, and a 3D facial scanner controls entry to the data centres. The buildings are video-monitored and visited by a security company at least four times per day outside of working hours.	We have made inquiries of Management about the procedures used. We have inspected all server rooms and ensured that all access routes are secured with a card reader.	No exceptions noted.

Control Objective C: Physical security

Operational management is carried out in premises that are protected from damage caused by physical conditions such as fire, water damage, power failure, theft or vandalism

Control objectives/control	PwC test	Result of test
Positioning and securing of equipment Inergen systems, temperature sensing and video surveillance are installed in the data centres. The Inergen systems are tested once a year according to current legislation. The test is carried out by RMG-Inspektion A/S, and an approved declaration exists. Management and the operating officer receive alarms both as SMS texts and e-mails in cases of possible incidents.	We have made inquiries of Management about the procedures/control activities performed. By inspection, we have reviewed the operation facilities and have confirmed that the necessary controls have been established in the form of: • Fire extinguishing systems • Humidity protection • UPS and generators • Physical access control systems • Indoor climate monitoring. Using random samples, we have inspected the documentation for equipment maintenance to confirm that it is being maintained on an ongoing basis.	No exceptions noted.
Support supplies (supply security) The data centres are protected against interruption to the power supply by the use of UPS. Diesel generators begin supplying power according to the set schedule. This is tested every month. Fuel levels are read on a regular basis.	We have made inquiries of Management about the procedures/control activities performed. By inspection of data centres, we have observed that Unit IT has established procedures for monitoring UPS and emergency power supplies. Using random samples, we have reviewed documentation of maintenance to verify that UPS or emergency power supplies are continuously maintained and tested.	No exceptions noted.
Securing of cables Cables and power are located in cable trays. Cross-connect and associated network devices are all found in the data centres.	By inspection, we have observed that cables for power supply and data communication are secured against damage and unauthorised modifications.	No exceptions noted.

Control Objective D: Communication and operation management

It is established that there are:

- *appropriate business practices and controls regarding operation, including monitoring, registration and follow-up of relevant events*
- *adequate procedures for backup and contingency plans*
- *appropriate function separation in and around the IT functions, including between development, operation and user functions*
- *appropriate business practices and controls regarding data communications that adequately secure against the risk of loss of authenticity, integrity, availability and confidentiality.*

Control objectives/control	PwC test	Result of test
Documented operating procedures Unit IT A/S has described operating procedures for the operating environment. A daily check of the server rooms is carried out. Then, a daily report is prepared that is approved by Management every day. Unit IT A/S has three different types of staff: support, operational and consultancy staff (storage, firewall and access control are part of operations). Access to common drives is assigned based on function. For each position, there is a job title. Unit IT A/S has no development or application maintenance.	We have made inquiries of Management about the procedures for documenting all relevant operating procedures. By inspection, we have observed that documented procedures exist in all relevant areas and that the documentation is compliant with the actual actions. Furthermore, we have observed that sufficient monitoring and follow-up are being carried out.	No exceptions noted.
Segregation of duties Management has implemented policies and procedures to ensure satisfactory separation of duties within the IT department. These policies and procedures require: • that responsibility for development and updates to the production environment is kept separate • that the IT department has no access to applications and transactions • that development and operational activities are kept separate.	We have made inquiries of Management about the procedures/control activities performed. We have reviewed users with administrative rights to verify that access is granted based on a work-related need. Using random samples, we have checked that the technical network has been segregated from the administrative network and that only relevant individuals can access the technical network.	No exceptions noted.
Measures against viruses and other malicious code Antivirus programs are installed and updated regularly. Unit IT A/S uses recognised antivirus software with automatic version control.	We have made inquiries of Management about the procedures/control activities performed. Using random samples, we have reviewed the technical set-up and observed that antivirus programs have been installed and are updated.	No exceptions noted.

Control Objective D: Communication and operation management

It is established that there are:

- *appropriate business practices and controls regarding operation, including monitoring, registration and follow-up of relevant events*
- *adequate procedures for backup and contingency plans*
- *appropriate function separation in and around the IT functions, including between development, operation and user functions*
- *appropriate business practices and controls regarding data communications that adequately secure against the risk of loss of authenticity, integrity, availability and confidentiality.*

Control objectives/control	PwC test	Result of test
Backing up of information Backup and validation are forwarded to Front-Safe A/S. One customer is selected in sequence every quarter for a test of the recovery procedure. Veeam is used for the backup/restore of virtual servers. Veeam is used as a disaster recovery backup, which only ensures that the system drives are in operation, and subsequently data on other drives is re-established with TSM. Veeam is used for a quick backup and installation and is continuously in operation according to agreement with the customer. It is regularly tested to determine if the backup is valid.	We have made inquiries of Management about the procedures/control activities that are being carried out, gone through backup procedures and confirmed that they are sufficiently and formally documented. We have received the agreement between Unit IT and Front-Safe A/S and observed that the backup procedure is in accordance with the uptime goals described in the contract. Using random samples, we have reviewed backup logs and observed that backups have been completed error-free or that corrections have been made in case of unsuccessful backups.	No exceptions noted.
Monitoring of system usage and audit logging Logging has been implemented on access to critical systems. These logs will be reviewed in case of suspicion of misuse or error. Unit IT A/S is not responsible for setting up and running the databases. All user privileges are checked at least once a year or upon the hiring of new employees or employees leaving. All hardware is monitored. A report is sent in the event of errors. Additionally, information boards have been set up that provide an overview of the installation. The monitoring system sends SMS texts and e-mails in cases of error. **Administrator and operator log** Unit IT A/S logs transactions and actions performed by	We have made inquiries of Management about the procedures/control activity performed. We have reviewed the system set-up on servers and major network devices, and using random samples, we have verified that parameters for logging have been established to log actions of users with extended rights. By inspection, we have observed that surveillance and alerts for reduced accessibility have been established, also for attempted breach of the established security measures. Using random samples, we have observed that adequate follow-up is made on logs from critical systems.	No exceptions noted.

Control Objective D: Communication and operation management

It is established that there are:

- *appropriate business practices and controls regarding operation, including monitoring, registration and follow-up of relevant events*
- *adequate procedures for backup and contingency plans*
- *appropriate function separation in and around the IT functions, including between development, operation and user functions*
- *appropriate business practices and controls regarding data communications that adequately secure against the risk of loss of authenticity, integrity, availability and confidentiality.*

Control objectives/control	PwC test	Result of test
users and administrators via domain controllers (AD) audit log. User account privileges are reviewed semi-annually. Logs from AD and other essential systems are reviewed on a continuous basis and by reason of suspected unauthorised actions.		

Control Objective E: Access control

It is established that there are:

- *appropriate business processes and controls for the allocation of, follow-up and maintenance of access rights to systems and data*
- *logical and physical access controls that limit the risk of unauthorised access to systems or data*
- *necessary logical access controls that support organisational separation of functions.*

Control objectives/control	PwC test	Result of test
User registration and administration of privileges The creation and deletion of users are the responsibility of the management group (MG). Users are created in relation to work-related needs. The procedure is approved by Management. All user privileges are checked at least once a year or upon the hiring or exit of employees. Access to customer systems is the responsibility of the customer. Therefore, Unit IT A/S has not described this. Users are created in groups. The privileges of these groups determine what the individual employee has access to. MG decides which groups an employee should be a member of. MG continuously assesses whether Unit IT A/S' employees have been given the correct privileges. All users in Unit IT A/S' AD and their privileges are reviewed at least four times a year.	We have made inquiries of Management about the procedures/control activities performed. We have reviewed the user administration procedures and have verified that the control activities are sufficiently comprehensive. Using random samples, we have verified that the creation of users and granting of access are documented and approved by MG in accordance with procedures. We have observed that annual reviews of user access and rights are conducted.	No exceptions noted.
Administration of user access codes (passwords) Programmed controls have been implemented ensuring that passwords are of the required quality in regard to the security policy provisions. A password must consist of at least 12 characters and the characters must be a mix of numbers and letters. A password is valid for a maximum of 60 days and should not be reused.	We have made inquiries of Management about the procedures/control activities performed in connection with password controls and verified that adequate authentication of users on all entries is ensured. Using random samples, we have tested that an appropriate quality of password is used in Unit IT A/S' operating environment by randomly testing that access to the company's system requires the use of a username and password.	No exceptions noted.

Control Objective E: Access control

It is established that there are:

- *appropriate business processes and controls for the allocation of, follow-up and maintenance of access rights to systems and data*
- *logical and physical access controls that limit the risk of unauthorised access to systems or data*
- *necessary logical access controls that support organisational separation of functions.*

Control objectives/control	PwC test	Result of test
Assessment of user access rights Unit IT A/S conducts periodic review of user privileges to ensure that these are in line with the user's work-related needs. Deviations are investigated and corrected in a timely manner.	We have made inquiries of Management about the procedures/control activities performed. Using random samples, we have controlled and verified that regular reviews are performed. Using random samples, we have furthermore verified that identified deviations are corrected.	No exceptions noted.
Revoking access rights User privileges for operating systems, networks, databases and data files concerning former employees are deactivated upon their resignation. Management approves the withdrawal of privileges and the deletion of users.	We have made inquiries of Management about the procedures/control activities performed to ensure that the withdrawal of access privileges is performed in accordance with satisfactory business procedures and that follow-up is completed according to the procedures for the assigned access privileges. Using random samples, we have checked that the procedures described are observed in relation to deactivated users on systems. Also, we have checked that inactive user accounts are deactivated upon resignation.	No exceptions noted.
Policy for the use of network services, including the authentication of users with an external connection All traffic to and from the internet is controlled via a firewall. The setup of this is electronically documented. Access from a home office is done using VPN. Customers have their own DMZ zone. External access from a home office or external partners is validated using "SSL-VPN".	We have made inquiries of Management about the procedures/control activity performed, and we have observed that an appropriate authentication process is being used for the operating environment. Using random samples, we have observed that users are identified and verified before access is given and that remote access is protected by VPN. By inspection, we have noted that the network is segmented into small networks using VLAN and DMZ to reduce the risk of unauthorised access.	No exceptions noted.

Control Objective E: Access control

It is established that there are:

- *appropriate business processes and controls for the allocation of, follow-up and maintenance of access rights to systems and data*
- *logical and physical access controls that limit the risk of unauthorised access to systems or data*
- *necessary logical access controls that support organisational separation of functions.*

Control objectives/control	PwC test	Result of test
Management of network connections Network connections are tested with the customer, if the customer so desires. Unit IT A/S reviews the firewall set-up to protect against unnecessary penetration. As a rule, it is closed to outside traffic. If customers want to change this, this is done by written request.	We have made inquiries of Management about the procedures/control activities performed to manage network connections. By inspection, we have noted that a periodic penetration test has been carried out and that identified weaknesses have been addressed. Through inspection, using random samples, we have reviewed the firewall configuration and checked that the firewall rules have been set up appropriately.	No exceptions noted.
Restricted access to information Only persons with access to customer-specific systems have access. All access requests for new and existing users regarding applications, databases and data files are reviewed to ensure compliance with Unit IT A/S' policies and that privileges assigned based on a work-related need have been approved and are properly set up in systems.	We have made inquiries of Management about the procedures/control activities performed to restrict access to information. We have reviewed the user administration procedures and observed that the control activities are sufficiently comprehensive. Through inspection, using random samples, we have tested that the granting of access to data and systems is carried out based on a work-related need and that access is approved in accordance with business procedures.	No exceptions noted.

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

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

Control objectives/control	PwC test	Result of test
Management of software on operating systems Unit IT A/S has separate development, testing and production environments. Unit IT A/S does not develop software. The IT environment for customer systems is separated from the internal IT environment. Unit IT A/S uses patch management to control, for example, the OS upgrade. Patching of customer servers is agreed to and accepted in collaboration with the individual customer. Patching is performed in the agreed service window. The procedure only involves the OS as the customer is responsible for the applications.	We have made inquiries of Management about the procedures/control activities performed to maintain separation between the individual environments. In addition, we have inquired Management about the procedures/control activities carried out to keep critical systems updated, and we have reviewed the adequacy of updating procedures in regard to Unit IT A/S' own major systems and customer systems in accordance with contractual agreements. Using random samples, we have reviewed the changes during the period and have verified that these are documented. In addition, using random samples, we have tested the controls, including whether: • there is sufficient communication with providers in order to receive necessary information about critical and important updates, as well as the necessary risk assessments of the individual updates. • the critical systems have been updated appropriately.	No exceptions noted.
Change management Unit IT A/S uses change management to control changes. Changes to daily tasks are described in standard changes, which are pre-approved. No changes to production are implemented before having been approved by the customer and Management, tested and before a fallback plan is prepared. Emergency changes beyond standard routine are tested and then approved. No change may be made without approval.	We have made inquiries of Management about the procedures/control activities performed, reviewed the adequacy of change management procedures and observed that an appropriate change management system has been established which is supported by a technical infrastructure. Using random samples, we have reviewed change requests for the following: • Registration of change requests in the established system • Documented test of changes, including approval • Approval must be obtained before implementation • Verbal approval by Management is considered sufficient for emergency changes, but must then be documented • Documented recovery plan, where relevant.	No exceptions noted.

Control Objective G: Contingency plan

Unit IT A/S is able to continue servicing customers in disaster situation.

Control objectives/control	PwC test	Result of test
Structure of disaster response Unit IT A/S has prepared a contingency plan. This describes probabilities as well as the necessary measures. The plan is approved by Management and reviewed annually. **Disaster response test** An annual test of disaster preparedness is carried out using both desktop tests and actual test scenarios. If the test reveals any discrepancies, the plan is immediately updated.	We have made inquiries of Management about the procedures/control activities performed. We have reviewed the material distributed on disaster recovery plans and verified that the organisational and operational IT disaster recovery plan contains managerial functional descriptions, contact information, task lists and instructions. Using random samples, we have checked that disaster recovery plans are tested through desk checks or realistic testing scenarios to the extent possible.	No exceptions noted.