www.pwc.dk

Unit IT A/S

Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 January 2023 to 31 December 2023 in relation to Unit IT A/S' operational services and hosting activities to customers

January 2024

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 B4RestoreA/S as a subservice supplier for backup storage. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore A/S performs for Unit IT A/S.

Some of the control objectives stated in our description in section 2 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with our controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

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

(iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to the 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 2023 to 31 December 2023. The criteria used in making this statement were that:

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

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

(iii) The controls were consistently applied as designed, including that manual controls were applied by persons who have the appropriate competence and authority, throughout the period from 1 January 2023 to 31 December 2023.

Middelfart, 9 January 2024
Unit IT A/S

Jess Julin Ibsen
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 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:

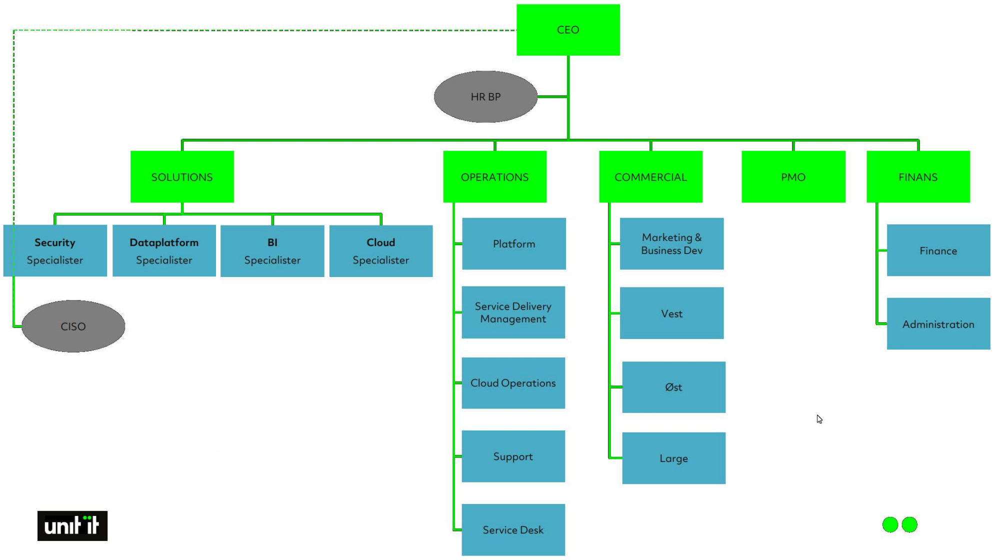
- Provision of private cloud services including the Windows operating system.
- High performance storage solutions.
- Customer-specific Remote Desktop and Citrix solutions.
- MS Exchange and Office365.
- Helpdesk and client support.
- SQL as a service.
- Image and remote backup.
- Security governing fully staffed operational 24/7 365 Cyber Defense Center.

Unit IT A/S currently has two data centres of its own in Middelfart and a co-location in Kolding, with approx. 24 km between the two data centres and the co-location. From here, approx. 3,000 servers are monitored and operated.

This description encompasses operations and monitoring from 1 January 2023 – 31 December 2023 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 the company 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, 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

The ISO 27000 series is used 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 is ISO27001 certified. The certificate is widely available from our website.

Our methodology for the implementation of controls is 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 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 we 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.

Unit IT A/S has approximately 50 employees and is headed by Managing Director Jess Julin Ibsen, who reports to the USTC group.

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

- Cloud Operation: 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: 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 and 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: 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.

  Security: The primary functions provided by the security teams, is to ensure that appropriate governance, risk management and compliance are in place and to guard information, system and networks from cyber-attacks (Cyber Defence Center). Security performs everything from maturity and risk assessments to 24/7 monitoring and technical security.

In addition, organisations exist for handling Sales & Marketing, SQL/BI and Finance (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 has formulated goals and actions in the current strategy, which aims to address external factors that could pose a risk to information security.

Policies and procedures, as part of our ISMS are widely available for all employees on SharePoint. An Information Security Policy has been formulated, 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.

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 to detect abnormal activity later.

Skill and competencies

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. Employee are expected to take relevant further education, which is arranged with the immediate superior. Unit IT A/S will bear all costs for this education. MUS interviews about education are held annually– 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.

Roles and responsibilities

The internal security function is carried out by the CISO in collaboration with management. This function ensures the implementation and updating of security and quality procedures, is responsible for the primary contact with external 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.

The responsibility for security policy, BCMS, 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

Management ensures 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 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 externals visiting our processing facilities 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 centers

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. Both centres have extended physical access control.

Both data centres can only 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. 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 centers

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 & 2:

- 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 an alarm centre with alarms for humidity, temperature, fire, UPS and emergency power generator.
- Service contracts on spare parts.
- Video surveillance.

Backup

Unless otherwise agreed, Unit IT A/S 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 virtual backup.

Virtual backup and disaster recovery

Disaster recovery backup is used to re-establish virtual servers very quickly in any data centre. Data can be restored in both our DC1 and DC2. All the data centres are connected with fibre for highest speed, 10Gbit between Kolding and Middelfart.

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 A/S 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 A/S encourages all customers to regularly validate the integrity of their backup data.

Unit IT A/S checks that all defined DR backups have been performed as planned, during weekdays. 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 investigated and evaluated.

By default, new virtual servers are included in the DR backup.

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 approximately 60 km away from Unit IT A/S' operating centre at B4Restore A/S in Stilling and Viby J. 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 A/S 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 Be4Restore's IBM Spectrum Protect backup servers and storage. Subsequently, the customer's data is copied to Be4Restore'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 Be4Restore A/S's backup servers.

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

Unit IT A/S carries out checks every weekday 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.

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

The change management strategy 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.
- 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.

Unit IT A/S follows a structured change management process and all changes are assessed and approve accordingly. All changes are categorized as either standard or normal changes. Standard changes, changes with a low impact, probability and classification are carried out without prior approval from the customer. Whereas normal changes are evaluated, send forward to the customer for approval, then scheduled and implemented according to a standardized process.

During service operation, we provide support for ongoing changes and releases to the IT services. This includes coordinating with the change management and release management processes to ensure that changes and releases are implemented smoothly and without causing disruptions. We collaborate with the development and testing teams to ensure that changes are properly tested, documented, and communicated to relevant stakeholders.

Access control

Access to IT-systems

The logical security includes protection of electronic systems and information's 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 aims to be a flexible workplace, which is why the ability to connect remotely is offered for our own as well as our customers' IT systems. To avoid unintended access, employees must lock or log off their personal computers when leaving the workplace.

Physical access to locations

Unit IT's office locations is under surveillance by an external alarm company. This company reacts to alarms and unforeseen events outside office hours.

Access options

Access to the administrative network and administrative systems is only available for authorised personnel and requires two-factor validation. Authorisation can only 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. Access to operational systems, are based on requirements for change via the ticket system, and the access granted is both logged and monitored.

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

Unit IT A/S has authorised mobile devices (smartphones, tablets mv.) to synchronise e-mails and calendars. No mobile devices can gain access to the management network nor operational systems. Access to data is controlled by the 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.

Credentials policy

Unit IT A/S' password policy requires at least 12 characters for normal users, 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 dictated by the customer access control policy.

Acquisition, 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.

A framework for transition to Unit IT A/S has been developed. The framework ensures a safe transfer of existing services from the customer's current vendor to the Unit IT A/S and the changes necessary to fulfil the requirements in the agreement.

The objective of the framework is to transfer services, knowledge and responsibilities from the incumbent vendor to Unit IT A/S, without losing availability of business and technical solutions, commencing a steady state of operation. This happens in a controlled way according to a mutually agreed transition plan, allowing for proactive risk mitigation and tracking of progress. Transition is a collaboration between Unit IT A/S, customer and incumbent vendor.

The framework consists of the following phases:

- establish a solid plan mutually agreed between all 3 (transition) parties,

- separate tracks to eliminate inter-dependencies,
- reduce risk impact and
- allow for one service tower to reach a steady state, even though the other is still pending finalization.

After a detailed transition plan has been mutually agreed upon, the transition is executed. Once Unit IT A/S feels confident that a satisfactory transition has been accomplished the customer executes a verification, upon which an acceptance (or rejection) can be issued. An acceptance can be full, partial or conditioned.

Management of security incidents

Unit IT A/S has as part of our ISO27001 certification implemented Information 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 both material and non-material security risks, and the security is maintained 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 governs its own fully managed Cyber Defense Center manned 24/7 365. The CDC correlates logs in our enterprise SIEM and utilises SOAR and threat intelligence to assess suspicious behaviour. Alarms are handled by a Tier1 and Tier2 setup. The Security department counts 13 FTE's.

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 together with Security who assesses what reaction is needed. Incidents outside normal working hours are handled by the SDM acting as Situation Manager, together with Security. If an incident occurs within normal working hours, the employee will handle and escalate the case in the same way as other cases and with the priority required.

All employees are obligated to report security breaches, suspicious events or activity to the CISO and Management immediately. Likewise, the company's monitoring system will be set up to identify security breaches.

Unit IT A/S has a formal process for identifying and risk assessing vulnerabilities. Based on several factors Security can call an 'out of band patch' if a risk is considered very high. An out of band patch must be applied within 4 hours.

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 (BCMS)

Information and communication

In accordance with the Business Continuity Management System (BCMS), Management is responsible for communication to customers and the press. The way things should be communicated is reflected in Unit IT A/S' BCMS, which includes telephone contact, SMS communications and e-mails in a structured communication platform used. 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 individual employees.

The BCMS policies and procedures used during activation of the BCMS is available in an offline version, for all employees on their laptops. 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.

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. Top management handles 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 ensures stakeholders are informed as soon as possible. Unit IT A/S has identified a preferred form of communication and roles and roles has been clearly defined. The BCMS policies and procedures used during activation of the BCMS is available in an offline version, for all employees on their laptops.

Communication preparedness, like technical preparedness, are rigorously tested as part of the BCMS.

Unit IT A/S considers minimum requirements for a viable hosting setup and uses procedures to ensure that we 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, creation and deletion of employees.

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.
- Ensure that systems that are operated can be patched and updated according to the manufacturer's instructions.
- Inform Unit IT A/S about the requirements for access management in connection with setting up and managing its own users in the production environment.
- If relevant, handle the set-up and administration of users from Unit IT A/S 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 A/S.
- Ensure that its own contingency plans include critical systems and also communicate which systems should be disaster recovery-tested and how often.

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 2023 to 31 December 2023 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 from 1 January 2023 to 31 December 2023 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

Unit IT A/S uses B4Restore A/S as a subservice supplier for applied backup storage. This report uses the carve-out method and does not comprise control objectives and related controls that B4Restore A/S performs for Unit IT A/S.

Some of the control objectives stated in Unit IT's description in section 2 can only be achieved if the complementary controls at customers are suitably designed and operating effectively with Unit IT's controls. This report does not comprise the suitability of the design and operating effectiveness of these complementary controls.

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.

Our firm applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service auditor's responsibilities

Our responsibility is to express an opinion on 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 suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by 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 2023 to 31 December 2023;

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

(c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2023 to 31 December 2023.

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used 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 misstatement in their financial statements.

Aarhus, 9 January 2024
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

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 2023 to 31 December 2023. Among other things, this includes assessment of patching level, permitted services, segmentation, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.
Reperformance of the control	Repetition of the relevant control. We have repeated the execution of the control to verify whether the control functions as assumed.

4.3 Control objectives, control activity, tests and test results

Control Objective 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 or Teams 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 performs supplier management. This involves a methodical identification of critical suppliers and sub processors, and a diligent evaluation of the supplier's current security posture in accordance to criticality. Furthermore Unit IT continuously monitors critical suppliers online presence in various forums on a daily basis.	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. This is done e.g., by ensuring that no single person is allowed to both create and approves changes, reducing the risk of unauthorized or inappropriate actions. These policies and procedures require: • Segregation of duties are implemented in the Change management process. All changes must be approved by change manager before implementation.. • Clearly defined roles and responsibility within each unit. • Elevation of admin rights are based on at least two users, one requestee and one approver.	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.

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
•		
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.
Backing up of information All backup data are forwarded to a third separate offsite Datacenter. • For Unit IT: Minimum once a year a test of the backup and recovery procedure for all business-critical systems is performed. • For customers: Restore tests are agreed individually based on e.g. criticality, frequency and retention period of systems and data.	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 B4Restore 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 Performance: All hardware is monitored. A report is sent in the event of an error. Additionally, information performance monitors located in Middelfart, Kolding and Aarhus in order to provide an overview of performance in the datacenters. Furthermore a text message is sent	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.	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
the to 24/7 operator on duty during out of business hours. Security: Logging has been implemented on access to critical systems and access to customer environments. These logs will be reviewed in case of suspicion of misuse or error. All logs are kept in accordance with Unit IT's policy for logging and monitoring. Logs are retained in tamper proof enterprise SIEM system. Unit IT's CDC actively responds to alarms 24/7 365. **Administrator and operator log** Any actions performed by any admin user or administrator via domain controllers (AD) is collected in an audit log. Changes performed by a privileged account is automatically notified to Security. New privileged users created will notify Unit IT's Security department. Extended conditional access rules from AD are reviewed at least quarterly. Any changes to CA rules will cause an alarm to Security by reason of suspected unauthorised actions.	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.	

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 user administration is the responsibility of the management group (MG). Users are created in relation to work-related needs. The procedure in accordance to Unit IT's Access Control Policy. All user privileges are reviewed at least once 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 symbols and letters. A password is valid for a maximum of 60 days and can't 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.	During our inspection of the Windows Servers we observed that 4 personal users have a password setting that means that it never expires as well as 2 personal users not having changed their password according to the maximum age policy of Unit IT. No further 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 performs annual review supplemented with internal audits 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 firewalls. The setup of this is electronically documented. Access to Unit IT's processing facilities from any external location is always done utilising always-on VPN. All access is subject to extended conditional access controls in order to prevent unauthorised access from an external location. Customers have their own DMZ zone.	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 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 customer information Only a very limited group of personnel has access to customer environments via dedicated personal accounts. Administering accounts follows Unit IT's access control policy and as such undergoes Internal audit by Security. Access is granted based on the specific job description. Tickets in TOPdesk with customer approval forms the basis of accessing customer environments. All access is logged. Each access is provided through a dedicated environment (Leveranceplatformen) utilising multiple layers of two factor validations. Access is only possible using a Unit IT certified device.	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.	We have observed that procedures for change management are not applied to all changes. No further 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.

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registereret, og informationerne er listet herunder.

"Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument."

Jess Julin Ibsen
Kunde
Serienummer: c51d4162-810e-4a38-8c1b-2deada7381a0
IP: 93.176.xxx.xxx
2024-01-09 12:10:48 UTC

Jesper Parsberg Madsen
PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231
Statsautoriseret revisor
Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e
IP: 83.136.xxx.xxx
2024-01-09 12:15:05 UTC

Penneo dokumentnøgle: AYQZA-8KA87-EF6DM-D3GCH-JVXYX-MKBBZ

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstemplet med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt
Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>.** Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**