www.pwc.dk

# *Mentor IT A/S*

## Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 April 2023 to 31 December 2023 in relation to Mentor IT's operating and hosting services to customers

*April 2024*

# Contents

# 1 Management's statement

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

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

Mentor IT confirms that:

a) The accompanying description in section 3 fairly presents the operating and hosting services that have processed customers' transactions throughout the period from 1 April 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 the operating and hosting services were designed and implemented, including:

- The types of services provided
- The procedures, within both information technology and manual systems, by which the IT general controls were managed
- Relevant control objectives and controls designed to achieve those objectives
- Controls that we assumed, in the design of the operating and hosting services, would be implemented by user entities and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description
- How the system dealt with significant events and conditions other than transactions
- Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities and monitoring controls that were relevant to the IT general controls

(ii) Includes relevant details of changes to IT general controls in relation to the operating and hosting services during the period from 1 April 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 operating and hosting services being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the IT general controls in relation to the operating and hosting services that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 April 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 April 2023 to 31 December 2023.

Esbjerg, 19 April 2024
**Mentor IT A/S**

Søren Frandsen
Executive Partner, Cloud & Infrastructure Growth

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

**Independent service auditor's ISAE 3402 assurance report on IT general controls during the period from 1 April 2023 to 31 December 2023 in relation to Mentor IT's operating and hosting services to customers**

To: Mentor IT, Mentor IT's customers and their auditors

### Scope

We have been engaged to provide assurance about Mentor IT's description in section 3 of its IT general controls in relation to the operating and hosting services which have processed customers' transactions throughout the period from 1 April 2023 to 31 December 2023 and about the design and operating effectiveness of controls related to the control objectives stated in the description.

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

### Mentor IT's responsibilities

Mentor 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 Mentor 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 its operating and hosting services and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein and the suitability of the criteria specified and described by Mentor 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

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

### Opinion

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

a) The description fairly presents how IT general controls in relation to the operating and hosting services were designed and implemented throughout the period from 1 April 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 April 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 April 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 Mentor IT's services and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Aarhus, 19 April 2024
**PricewaterhouseCoopers**
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Jesper Parsberg Madsen
State-Authorised Public Accountant
mne26801

Iraj Bastar
Director

# 3 Service organisation's description

## 3.1 Overview

The purpose of this description is to inform the customers of Mentor IT and their auditors about the systems in place at Mentor IT and to ensure that the requirements of "International Standard on Assurance Engagements 3402" and "Assurance Reports on Controls at a Service Organisation" have been met. The description has also been made to inform about the controls in use to ensure safe and stable operation of the cloud services (CS), rack hosting services (RS) and support services (SS) delivered to Mentor IT A/S's customers.

Sotea A/S has become a part of Mentor It A/S during 2023. This audit report contains previous Sotea customers after they have been migrated into the Mentor It A/S' services and IT controls.

## 3.2 Mentor IT A/S and description of services

Mentor IT was founded in 1999 and is located in Esbjerg, Kolding, Aarhus and Ballerup, Denmark. Mentor IT specialises in IT outsourcing offering cloud solutions and managed services to companies. These services include cloud solutions, back-up solutions, IT security solutions , IT maintenance solutions and service desk solutions.

The facilities include two secure data centres in Esbjerg. Both data centres are owned by Mentor IT and are located more than five kilometres apart and connected through redundant fibre optics. All server systems are placed in Denmark, and redundant fibre connections from TDC, GlobalConnect and Norlys with very high bandwidth ensure that customers are provided with a quick and reliable solution.

Mentor IT is a well-established company respected within the Outsourcing and Managed Service Provider business. The services offered are based on world-leading products and "best practices", intending to ensure that customers are offered the best possible solutions and that they are not technologically bound to Mentor IT.

Mentor IT focuses on high quality and secure solutions, which their membership of and a quality certificate received from the Danish Cloud Community (DCC) confirms.

The solutions offered by Mentor IT are developed to support the customers' businesses in certain key areas:

- Controlling business processes
- Increasing business efficiency
- Increasing productivity
- Increasing benefit from IT solutions.

### 3.2.1 Description of services

Below, the controls in use regarding cloud services (CS), rack hosting services (RS) and support services (SS) delivered by Mentor IT are described. The services offered by Mentor IT are referred to as Mentor IT, which covers CS, RS and SS. The services delivered by Mentor IT are described focusing on the established controls relevant to the ERP system platforms of Mentor IT A/S's customers.

The intention of the description is to include most of the customers of Mentor IT. Thus, focus is on the processes and controls relating to the common services of Mentor IT. Specific services or settings relating to individual customers are not included in this description, but they are defined in the customer contract. This statement therefore only includes equipment located at the Mentor IT data centres.

Mentor IT delivers a range of services from web hotels to service agreements. Below is a list of some of these services, which are also described in the section following it.

- Cloud services (CS), including services such as:
  - Server platforms
  - Web hotel and DNS hotel
  - Email scanning
  - Backup solutions
  - Hosted Infrastructure
  - Maintenance
  - Surveillance

- Rack hosting (RH), including services such as:
  - Facility
  - Infrastructure

- Support services (SS) such as:
  - Regular maintenance
  - Service agreements
  - Regular consultancy work on services included in the agreement.

#### 3.2.1.1 Cloud services (CS)

Cloud services are developed as an alternative to the traditional on-site servers and server functions owned and maintained by the customer. These services are operated in the data centres of Mentor IT based on a set of standard services. Customers can choose which services their companies need and only buy those necessary.

- Mentor IT A/S delivers the software for the operating systems. Back-up copies are made of all data and configurations according to the customers' choices are specified in their contracts. Service level agreements (SLAs) exist.

- For the individual customer systems, the customers are allowed to bring third-party software.

- The systems are operated on a common hardware platform.

- Mentor IT is responsible for any administration and control of the hardware platform. The level of support and access to the systems follow the contract and the SLA.

#### 3.2.1.2 Rack hosting (RH)

Customers with a request or demand for operating their own hardware platform can use Mentor IT's rack hosting services, with "renting" server room facilities. Rack hosting covers services such as cooling, generators, UPS, fire extinguishing system, power, surveillance, infrastructure, alarm system, documentation and the rack itself.

- The rack is supplied and maintained by Mentor IT.

- Power and cooling are supplied and maintained by Mentor IT.

- Server room environment monitoring is managed by Mentor IT.

- Access control and surveillance is managed by Mentor IT.

- Infrastructure can be supplied by Mentor IT, but customers are allowed to bring their own fibre connections.

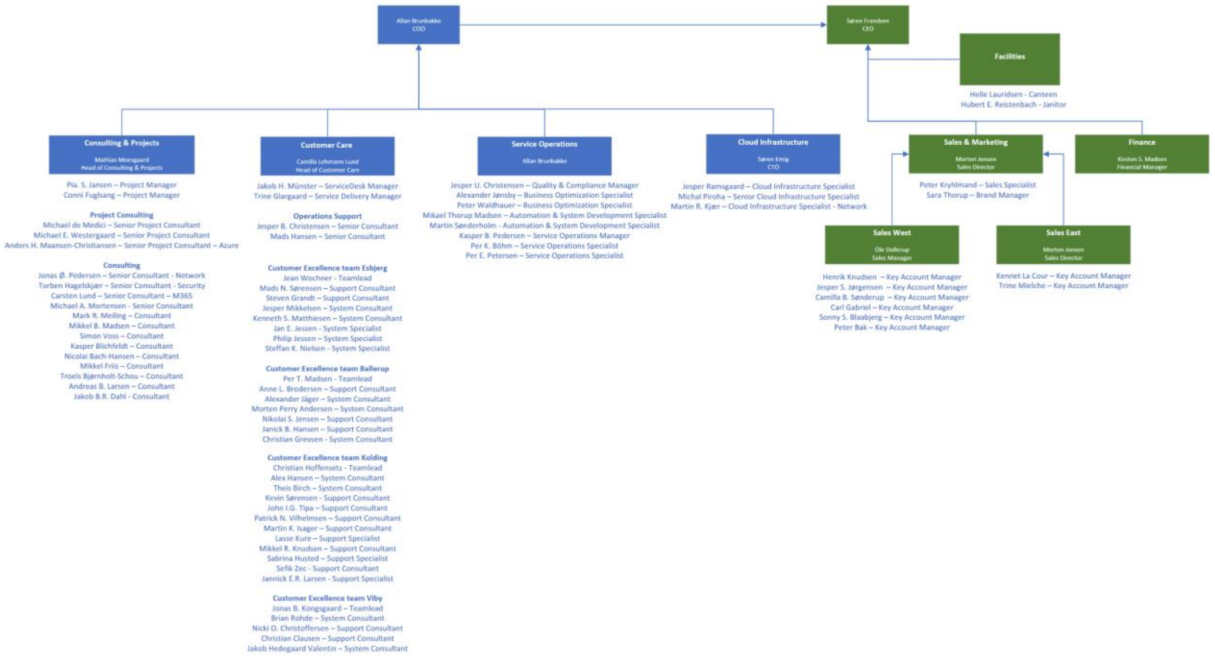
### 3.2.1.3 Support services (SS)

Support services are offered as an add-on to the customer's solutions. The support services can be maintained on the customer's solution, with patches being installed and regular maintenance work being performed. Support Service can also include user support on applications. Furthermore, these services can be bought on an hour-to-hour basis for new projects, installation of new software, change of user rights, new users, etc. The required amount of Support Services for a customer is based on the customer's individual need for support.

- A maintenance agreement offers installation of security patches to the operating systems
- A service agreement offers installation of security patches to the operating systems and other Microsoft applications, but also user support according to the specifications in the contract
- Other services can be bought per project or per hour.

## 3.3 *Mentor IT A/S's organisation and security*

The organisational chart below shows the organisation and responsibilities of Mentor IT A/S.


Allan Brunbakke
COO
Søren Frandsen
CEO
Facilities
Helle Lauridsen - Canteen
Hubert E. Reistenbach - Janitor
Consulting & Projects
Mathias Moesgaard
Head of Consulting & Projects
Pia. S. Jansen – Project Manager
Conni Fuglsang – Project Manager
Project Consulting
Michael de Medici – Senior Project Consultant
Michael E. Westergaard – Senior Project Consultant
Anders H. Maansen-Christiansen – Senior Project Consultant – Azure
Consulting
Jonas Ø. Pedersen – Senior Consultant - Network
Torben Hagelskjær – Senior Consultant - Security
Carsten Lund – Senior Consultant – M365
Michael A. Mortensen - Senior Consultant
Mark R. Meiling – Consultant
Mikkel B. Madsen – Consultant
Simon Voss – Consultant
Kasper Blichfeldt – Consultant
Nicolai Bach-Hansen – Consultant
Mikkel Friis – Consultant
Troels Bjørnholt-Schou – Consultant
Andreas B. Larsen – Consultant
Jakob B.R. Dahl - Consultant
Customer Care
Camilla Lehmann Lund
Head of Customer Care
Jakob H. Münster – ServiceDesk Manager
Trine Glargaard – Service Delivery Manager
Operations Support
Jesper B. Christensen – Senior Consultant
Mads Hansen – Senior Consultant
Customer Excellence team Esbjerg
Jean Wochner - Teamlead
Mads N. Sørensen – Support Consultant
Steven Grandt – Support Consultant
Jesper Mikkelsen – System Consultant
Kenneth S. Matthiesen – System Consultant
Jan E. Jessen - System Specialist
Philip Jessen – System Specialist
Steffan K. Nielsen - System Specialist
Customer Excellence team Ballerup
Per T. Madsen - Teamlead
Anne L. Brodersen – Support Consultant
Alexander Jäger – System Consultant
Morten Perry Andersen – System Consultant
Nikolai S. Jensen – Support Consultant
Janick B. Hansen – Support Consultant
Christian Grevsen - System Consultant
Customer Excellence team Kolding
Christian Hoffensetz - Teamlead
Alex Hansen – System Consultant
Theis Birch – System Consultant
Kevin Sørensen - Support Consultant
John I.G. Tipa – Support Consultant
Patrick N. Vilhelmsen – Support Consultant
Martin K. Isager – Support Consultant
Lasse Kure – Support Specialist
Mikkel R. Knudsen – Support Consultant
Sabrina Husted – Support Specialist
Sefik Zec - Support Consultant
Jannick E.R. Larsen - Support Specialist
Customer Excellence team Viby
Jonas B. Kongsgaard – Teamlead
Brian Rohde – System Consultant
Nicki O. Christoffersen – Support Consultant
Christian Clausen – Support Consultant
Jakob Hedegaard Valentin – System Consultant
Service Operations
Allan Brunbakke
Jesper U. Christensen – Quality & Compliance Manager
Alexander Jønsby – Business Optimization Specialist
Peter Waldhauer – Business Optimization Specialist
Mikael Thorup Madsen – Automation & System Development Specialist
Martin Sønderholm - Automation & System Development Specialist
Kasper B. Pedersen – Service Operations Manager
Per K. Böhm – Service Operations Specialist
Per E. Petersen – Service Operations Specialist
Cloud Infrastructure
Søren Emig
CTO
Jesper Ramsgaard – Cloud Infrastructure Specialist
Michal Piroha – Senior Cloud Infrastructure Specialist
Martin R. Kjær – Cloud Infrastructure Specialist - Network
Sales & Marketing
Morten Jensen
Sales Director
Peter Kryhlmand – Sales Specialist
Sara Thorup – Brand Manager
Finance
Kirsten S. Madsen
Financial Manager
Sales West
Ole Dollerup
Sales Manager
Henrik Knudsen – Key Account Manager
Jesper S. Jørgensen – Key Account Manager
Camilla B. Sønderup – Key Account Manager
Carl Gabriel – Key Account Manager
Sonny S. Blaabjerg – Key Account Manager
Peter Bak – Key Account Manager
Sales East
Morten Jensen
Sales Director
Kennet La Cour – Key Account Manager
Trine Mielche – Key Account Manager

## 3.4 *Risk assessment*

Mentor IT's Management is responsible for identifying the risks and for establishing the required level of control to avoid those risks. This includes controls on the systems, facilities and infrastructure in Mentor IT's data centres in Esbjerg.

The members of Management convene on a regular basis to discuss the business risks, including the financial and technical risks. Regular meetings attended by Management and employees are held to discuss current projects, system maintenance, education and new products in order to provide general information and identify potential risks.

On a yearly basis, the control team carries out a risk assessment of the systems and businesses of Mentor IT. The theory used for assessing the risks in the systems and businesses is based on a matrix of "consequence of the risk multiplied by the probability of the risk happening". The risk assessment takes both internal and external factors into consideration as well as Management's ability to focus on the impact of these factors. The risk assessment is published for Management and the Board of Directors.

## 3.5 Control framework, control structure, and criteria for control implementation

The following principles and criteria were used for producing the description of the systems in place at Mentor IT. The same principles were also used for assessing whether the controls had been developed suitably and whether the controls are implemented in the organisation.

As a member of DCC, Mentor IT is also subject to an annual system / IT audit which results in an annual auditor's report prepared in compliance with ISAE3402.

The determination of criteria for control implementation at Mentor IT is based on ISO 27001/27002:2013. Based on this control framework and best practice, control areas and control activities have been implemented to minimise the risk of services provided by Mentor IT. Based on the control model selected, the following control areas are included in the overall control environment:

- Information security policies
- Organisation of information security
- Human resources security
- Access control
- Physical and environmental security
- Operations security
- Communications security
- Systems acquisition, development and maintenance
- Information security incident management
- Information security aspects of business continuity management.

## 3.6 Control environment established

Each area is described in detail in the sections below.

### 3.6.1 Information security policies

A formal IT policy is in place. The control team and Management have designed the policy in order to include both technical and company policies. On a yearly basis, the policy is reviewed.

### 3.6.2 Organisation of information security

The information security and control environment of Mentor IT reflects the stand taken by Management and the Board of Directors on the importance of controls and the impact on controls in politics, procedures, methods and the organisational structure.

#### 3.6.2.1 Responsibilities

The Board of Mentor IT is responsible for respecting Mentor IT's business policies. The Board consists of internal and external directors, who convene at least once every quarter to discuss the issues regarding the general operation and the finances of Mentor IT.

The board is responsible for reviewing the following:

- The financial results of Mentor IT
- Reports from auditors regarding financial and IT security
- The observations and recommendations made by the control team.

### 3.6.2.2 Authorities

Mentor IT is registered at DK-CERT in order to help respond to IT threats and IT crime.

### 3.6.2.3 Control team

A control team has been set up at Mentor IT. The control team has unlimited access to reviewing the business of Mentor IT in order to ensure compliance with procedures. The control team reports directly to Mentor IT's Management.

The purpose of the control team is to assist Management in complying with its responsibilities concerning:

- The internal controls regarding the data centres' operational systems;
- The internal controls regarding procedures.

The control team will contribute to continuous improvement of the company policies, procedures and practices at all levels.

### 3.6.2.4 External parties

Mentor IT is independent of its suppliers and customers, both organisationally and functionally.

Procedures are in place to allow the customer to designate an "Approver" who bears the responsibility of validating modifications to user rights. The same Approver must also approve third-party supplier's access to services.

Whether to use the approver workflow is optional for the customer.

## *3.6.3 Human resources security*

The recruitment procedures of Mentor IT have been standardised. When recruitment is required, Human Resources posts the available position, including a description of the tasks and responsibilities related to the position. The candidates are reviewed in terms of qualifications, and interviews are held. Whether a job offer is made depends on the candidate's qualifications, references, personality and criminal record.

The HR policies and procedures are available from the corporate intranet.

The policies include:

- Equal treatment
- Codes for business responsibility
    - Ethical standards
    - Honesty and fair treatment
    - Conflicts of interest
- Publication, use, and copyright of Mentor IT's software or third-party software
- Harassment
- Confidentiality
- IT communication systems.

The values of Mentor IT are available on the corporate intranet. The employees are to create value for the customers, be responsible, react to issues, communicate in an understandable way and commit themselves to their jobs.

All new employees of Mentor IT are required to participate in an introduction programme. This programme provides information about the general policies, procedures and organisation of Mentor IT and allows for new employees to familiarise themselves with the business philosophy.

Mentor IT has implemented various communication methods to help its employees understand their individual roles and responsibilities, and controls, and to help them ensure that important incidents are communicated in a timely manner. They include:

- Guidance programmes for new employees and existing employees who experience a change in their job description. New employees go through the policies of Mentor IT as part of the information process.

- News channels and memos provide information about important incidents and changes to company policies and are published regularly. Urgent information is communicated to the employees by news channels or email.

- Staff meetings are held once a month or when necessary. These meetings offer the employees the opportunity to ask questions about the standard policies or exceptions to them.

All employees are entitled to vacation as specified in their contracts of employment. The vacation must be approved by the supervisor. Upon retirement and employee termination, interviews are held, and the company's property is collected. Standard procedures are in place for the collection of company property, and deactivation of access keys and logins.

Mentor IT has a policy on equal treatment of men and women which all employees must be aware of.

The ethical standards of Mentor IT serve as a guideline for all employees in matters concerning customers, the public, suppliers and colleagues.

### 3.6.4 Asset management

The data centres of Mentor IT are operated according to a 'Best-of-Breed' policy by only using hardware, software and middleware from leading manufacturers in the market, for example: NetApp, Lenovo, HP, Juniper, VMware, Veeam, Brocade, APC, Microsoft, Linux, Cummins Diesel generators and Autronica. This ensures reliability and compatibility.

Examples of equipment in use:

- Blade servers
- SAN systems
- Fibre switches
- Data centre switches
- Software for virtualisation
- UPS
- Monitoring system
- Diesel generator
- Fire extinguishing equipment.

All equipment is registered to and owned by Mentor IT. The only exceptions are:

- Specific software licences that can only be delivered to customers as a service:
  - For these licences, service provider agreements have been made between Mentor IT and the manufacturer.

- Customer hardware in the rack hosting service.

Only equipment approved by Management can be used for Mentor IT's services.

## 3.6.5 Access control

### 3.6.5.1 Business requirements for access control

Procedures for access control are in place. Access to managing Mentor IT's systems requires approval from Management, who also defines which systems should be accessible by the employees. Access rights are pre-approved based on three fixed user groups that reflect the group's work-related needs.

The Cloud Infrastructure team is responsible for developing standards and administering logical safety for the employees of Mentor IT on selected systems and applications. All Mentor IT's customer environments are kept separate.

User IDs and passwords for infrastructure, platform and most applications have internal settings which allow a predetermined number of invalid access attempts before they are deactivated. Involvement of the Cloud Infrastructure team is necessary if a password has been deactivated.

Mentor IT's Management checks personnel access granted. User access is updated by the Cloud Infrastructure team.

Access to the systems at Mentor IT is based on rights given to a domain user. This means that termination of employees only requires disabling of the domain user. Then access to Mentor IT's network and systems is prohibited.

### 3.6.5.2 User access management

User accounts are set up according to a process, with Management informing the Cloud Infrastructure and the Service Operations team of new employees. The manager of the new employee defines the level of access based on the employee's job description and role. Checks if access to HS systems is conducted by the CTO.

The employees of Mentor IT may need access to Mentor IT's customer systems for maintenance or support purposes. This is made possible through logical access groups providing access to both servers and passwords.

Logical access control is conducted according to the associated SOP for this.

### 3.6.5.3 User responsibilities

Employees are required to follow the password policy as stated in the IT policy of Mentor IT.

Mentor IT informs customers and their users about password policies when creating new users.

### 3.6.5.4 Controls to be performed by the customer

The controls of Mentor IT have been designed based on the assumption that certain controls are performed in-house by the customer. Implementation by the customer of these internal controls is necessary to ensure the level of security specified by Mentor IT in this document.

The controls referred to below are considered the minimum level of controls that a customer is required to have to ensure the level of security specified in this document. The list is not exhaustive, as it depends on the customer's transactions:

- **Access control**: The customer is responsible for implementing and administering access control to ensure that it prevents unauthorised access to applications and data.

- **System access**: The customer is responsible for ensuring that access to data and applications includes formal control of user identification, access rights, and logging of additions, deletions, and changes to access controls. The control must also include periodic reviews of user access rights to ensure that access to data is appropriate with regard to user responsibility and job function.

- **Incident management:** The customer is responsible for reporting all incidents that may affect the operating systems.

- **Change management**: The customer is responsible for specifying and recognising the need for testing new patches and the authorisation of new patches in their environments.

## *3.6.6 Physical and environmental security*

### 3.6.6.1 Security – physical access

Mentor IT has formal policies and procedures in place for access control of facilities and data centres. These policies and procedures define the levels of access, referring to the classification of employees, and describe the permits required to obtain and survey access.

### 3.6.6.2 Administration of access control

The entrances to the data centres are secured by key cards, which are connected to a central alarm unit. Access to facilities is granted based on job responsibility and is administrated by Management according to internal procedures.

### 3.6.6.3 Surveillance

The entrances to the data centres are equipped with alarms and video surveillance. Video activity is transferred to a central server and is kept on SAN. Any access to the data centre is monitored so that controlled/authorised access is maintained. Regular controls are performed to ensure that the list of employees who are granted access is up to date. Technicians in need of access due to business errands will be escorted.

### 3.6.6.4 Physical security measures

Physical security measures and control systems are in place to protect the data centres of Mentor IT against the surroundings. These systems include:

- Climate control in the data centres – HVAC (Heating, Ventilating, and Air Conditioning) systems – are monitored by Mentor IT personnel 24/7. Alarms inform employees of conditions which deviate from predetermined temperatures or levels of humidity. The employees respond to alarms and rectify the problem, if necessary.

- Heat and smoke detectors are mounted in the ceiling and under the elevated floor. A Senator 100 device alerts and activates Aragonite fire-extinguishing equipment in case of fire.

- HVAC and fire detectors are tested at least once a year.

- Preventive groundwater protection has been installed, and alarms are in place to notify Mentor IT before reaching critical levels in the event of failure of these systems. These alarms are tested every time the generator and UPS are tested.

- Power Supply and back-up facilities are installed and maintained to ensure a continuous supply of electricity in case of a power cut. These systems include an Uninterruptible Power Supply (UPS), Power Distribution Units and generators. UPS systems generate approx. 10-20 minutes of continuous electricity to ensure proper closing down of the system, if necessary. The data centres are also equipped with back-up diesel generators which can be used for protecting the data centres and the facility from irregularities in the electricity supply and aid in case of a major power supply issue. UPS systems and generators are tested periodically to ensure they are fully functional.

Cables and cords connected to or coming from IT equipment and peripheral units are placed outside of normal walking areas. Cables for IT equipment are placed under an elevated floor or in a circuit under the ceiling.

Equipment outside of the building is protected by a fence and monitored by way of video cameras.

Hardware no longer in service is stored for a certain period prior to its destruction.

## *3.6.7 Operations security*

### 3.6.7.1 Standard operating procedures

Procedures are in place for operating systems and services at Mentor IT.

### 3.6.7.2 Change management

A change management system is used for ensuring that changes to the services offered by Mentor IT are approved by Management and carried out in the best possible way.

### 3.6.7.3 Backup of operational systems

Backup of all Mentor IT servers is conducted daily. The image-based backup is performed to storage in data centre 2. Furthermore, documentation of all Mentor IT systems is located on Microsoft Office 365 and is backed up to facilities in Denmark. IP address management (IPAM) is backed up to the secondary data centre.

All back-up reports are sent to the back-up team for monitoring according to the SOP.

### 3.6.7.4 Backup of customer environments

Based on either the customer's backup agreement or Mentor IT default configuration, backup is conducted on a daily basis.

Backup protects the customer's data or systems in terms of integrity and security. Depending on customer requirements, backup is either conducted every hour or night or at another scheduled point in time through an automated process.

Three types of backups are available:

- Data backup
- Office 365 backup
- Image-based backup (snapshot backup).

Using the product "Data backup", backup copies are made of selected files and/or databases. When using this product alone, it is not possible to restore a server from the backup. A basic installation is required to restore data from the backup. The customer can be granted access to the backup client and is able to restore and select files for backup. Configuration of several backup jobs with different histories is also an option.

Data backup data are stored at an external provider, while Mentor IT retains responsibility for the operational aspects of the backup process, such as monitoring backup jobs, taking necessary actions based on backup reports and performing restore tests regularly.

Office 365 backup backs up emails, data in SharePoint and Teams.

"Image-based backup" offers backup of the complete server, and with this product it is possible to restore the complete server as it was when the backup was made. Normally, a 7-day backup history is used, but this may vary. The customer is not granted access to the backup product. Restoring files or systems is only possible through the support team of Mentor IT. Customer-specific requirements regarding backup history can be arranged. The image-based backup is stored at Datacenter 2.

It is possible to combine the three products for optimum data security.

### 3.6.7.5 Logs

Mentor IT has implemented an audit system to ensure visibility and control of our internal management infrastructure in order to quickly identify suspicious behaviour and investigate it thoroughly.

The solution is automated and offers reports and alerts based on changes in and activities from Active Directory objects and group policies. This allows Mentor IT to:

- Identify potential threat actors
- Assess and mitigate IT security risks
- Respond quickly to threats
- Investigate anomalies in user behaviour.

The customers' operational systems are installed with standard logging of system events, application events and user events. Back-up copies are made of these logs according to the back-up agreement between Mentor IT and the customer.

### 3.6.7.6 Monitoring

The operational environment of Mentor IT is constantly monitored by several monitoring systems. One of these systems is the primary monitoring system for all Mentor IT systems and services, but some systems are also monitored directly from the manufacturer.

*The primary monitoring system*

The primary monitoring system is configured to sending notifications if predetermined parameters are deviated from. These parameters are defined at a level where the notification will arrive in time for the incident to be solved within opening hours without escalating the incident. Another predetermined set of parameters will activate a warning in the event of deviation.

The individual customer systems are monitored on general parameters, including but not limited to the level of free disk space and the level of uptime.

Customers can buy additional monitoring with several reaction options.

*Other monitoring systems*

Some systems are monitored directly from the manufacturer. An example of this is the 3PAR & NetAPP storage systems which are monitored 24/7/365 by the manufacturers according to the service contract. The manufacturers will contact Mentor IT in case of incidents.

*Logging of errors*

The primary monitoring systems log all notifications for one year according to the SOP.

*Time servers*

Where possible, all services are configured to synchronise with standard time servers on the internet.

### 3.6.7.7 Responsibilities

The management and delivery of Mentor IT services is carried out by several teams of Mentor IT as defined in the organisation of Mentor IT, see section 3.3.

*Cloud Infrastructure team*

The Cloud Infrastructure team is responsible for maintaining all hardware stored at the data centres of Mentor IT, including repair and replacement. The equipment of customers using rack hosting services is not included in the maintenance program. This team is also responsible for ensuring a reasonable store of spare parts for hardware used in providing Mentor IT services and that service contracts are in place for all relevant equipment.

*Service & Operation team*

The Service & Operation team is responsible for the daily activities regarding monitoring, planning, problem solving and backup of systems and data for customers. The team ensures that the activities are planned and carried out according to the formal procedures and practices, and that any problem is traced, registered and solved. Problems regarding operations are logged according to the SOP, so that recurring problems are easily identified.

Examples of problems could be partly failed backup of asset, failed patching, etc.

*Consulting & Projects team*
The Consulting & Projects team is responsible for creating, supporting and implementing a standardised, secure infrastructure for the customers who are using Mentor IT services, ensuring a stable and highly available solution.

*Customer Care team*
The Customer Care team of Mentor IT offers support on all Mentor IT services. Support is offered when incidents are reported by phone or email or triggered by alarms. The support includes investigation and resolving of technical and system-related incidents. All incidents are logged in the service management system. Support services are invoiced according to the individual customer contract. The support team also maintains the systems of customers with a maintenance or service agreement.

Mentor IT offers the option to receive support outside of opening hours by simply calling Mentor IT and choosing the relevant option on the answering machine. This service is available to everyone; however, the support is not necessarily free of charge since it depends on the incident and the individual customer's contract.

### 3.6.7.8 Third-party delivery management

Whenever a major deviation in a contract between Mentor IT and a supplier occurs, the supplier will be contacted, and the deviation corrected. If this is not possible, the supplier will be replaced.

### 3.6.7.9 System planning and acceptance

Formal information and reporting systems have been implemented to ensure that Management is able to monitor key performance indicators. Each business unit has and maintains reporting systems that provide appropriate information about the processes for which they are responsible.

When capacity usage is approaching 80%, Management will be informed thereof. All systems in Mentor IT are scalable, making purchasing and installation easy. New technology is implemented by a group of experts who design, implement and test the technology before it is put into operation.

## *3.6.8 Communications security*

### 3.6.8.1 Network security management

Mentor IT collaborates closely with several suppliers of fibre broadband in order to deliver cost-effective and scalable connections from the customers' business location to the data centres of Mentor IT. Mentor IT collaborates with Fortigate, Cisco & Juniper, using their latest technology in the design and implementation of switches, routers and firewalls. Mentor IT delivers detailed network monitoring and control systems to maintain and monitor the services. Customers are able to purchase access to these systems if they want to monitor the systems themselves.

Mentor IT is a member of RIPE NCC (LIR agreement) and "owns" its own segment of IP addresses. This makes Mentor IT independent of internet service providers, allowing them to switch between suppliers should fibre connections from one company fail. Only Management and the team leader of Mentor IT have access to the RIPE NCC services.

Mentor IT connects the customer's business locations and the data centres of Mentor IT through secure connections. MPLS, VPN, and EPL are among the most used connection types for the data centres. Back-up traffic is encrypted.

Internet and MPLS access are provided through redundant fibre solutions offered by multiple internet service providers. These connections are kept physically separate until connected to the network. Combined with their own BGP routing, this makes Mentor IT truly independent of a single internet service provider.

By ensuring that servers and relevant resources are configured in a separate virtual local area network (VLAN), the network of each customer is physically and logically secured. The only transaction-related traffic allowed on the customers' servers is specific to the customers' employees and the support team of Mentor IT.

Customers can buy service and maintenance for their routers, but this is not a requirement. Should one customer suffer from a network failure due to old firmware of the router, this will not affect other customers of Mentor IT.

The infrastructure of the data centres is reviewed on a regular basis to ensure that the customers' needs, and requirements are fulfilled.

## *3.6.9 Systems acquisition, development, and maintenance*

New hardware or systems to Mentor IT is discussed and tested by the Cloud Infrastructure team before approval by Management.

Existing hardware or systems are maintained according to the manufacturer's recommendations.

### 3.6.9.1 Patch management

For service agreements including the service "vedligehold / patch management", Mentor IT will perform patch management on behalf of the customer. This service is defined as a service from Mentor IT, with relevant patches, evaluated by employees of Mentor IT, being installed on operating systems and MS Office products on the customer's servers.

Mentor IT monitors the update status of the servers according to the period defined in the agreement.

Patching of network equipment in data centres is done based on an evaluation of the relevant firmware/software. The Cloud Infrastructure team at Mentor IT monitors releases of firmware for the network equipment and applies relevant updates.

### 3.6.9.2 Protection against cybercrime

To ensure maximum security, all customers are offered several protection mechanisms against cybercrime. All new contracts (unless otherwise agreed) include image-based backup to ensure protection of data and a reduced "return to operation time" in case of an incident.

To reduce the risk of an incident, customers are offered advanced spam filter configuration to reduce the threat of cryptoware/ransomware and prevent CEO Phishing. Customers are also offered an additional layer of security (Secure DNS or similar) to prevent incidents from occurring in the event of a user activating a cryptoware link.

All internet connections are monitored to prevent customers from being affected by DDOS. In case of DDOS, the internet traffic of the specific IP address(es) is routed to a "black hole" in cooperation with the internet service provider(s).

## *3.6.10 Information security incident management*

### 3.6.10.1 Reporting information security events and weaknesses

All incidents involving the platform and services of Mentor IT are reported to Management and logged according to the SOP. There are no formal requirements as to the form of the report to be presented to Management except in the event of major incidents.

Mentor IT has implemented several communication methods to ensure that the customers understand the roles and responsibilities of Mentor IT and to inform about incidents as soon as possible. These methods include immediate reports to customers, regular notices in the newsletters from Mentor IT, and project managers who keep in contact with the customers' representatives and update them on new subjects and developments.

#### 3.6.10.2 Management of information security incidents and improvements

Major incidents are assessed, and root causes must be identified. Based on the incident and root cause, Management and the technical team decide on changes to avoid the recurrence of such an incident in the future.

### 3.6.11 Information security aspects of business continuity management

To ensure the continuity of Mentor IT, a contingency plan is in place. This plan describes and sets forth guidelines on how to manage an emergency.

Among other things, the contingency plan describes how to determine whether to continue operation in the data centres in Esbjerg or to establish operations elsewhere. It also includes checklists, contact lists, and procedures to ensure the contingency of Mentor IT.

The contingency plan is tested every two years with participation of relevant employees.

Findings and improvements are discussed with Management, and the contingency plan is brought up to date.

## 3.7 Complementary user entity controls to be considered by the customer's auditors

### 3.7.1 Services provided

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

Some of the control objectives described in Mentor IT's description of its system can only be achieved if the complementary controls at the user organisations are suitably designed and operating effectively together with the controls at Mentor IT. This includes complementary user entity controls described in the following:

#### 3.7.1.1 Access management

Mentor IT performs access provisioning in accordance with customer instructions, covering:

- Logical access for customers and third-party consultants used by the customer
- Physical access to data centres.

Customers are responsible for ensuring that an appropriate process for access provisioning for logical access and physical access is implemented and that the information provided to Mentor IT is correct. The customers are also responsible for ensuring that the access rights assignments for applications are provided adequately and in compliance with best practice for segregation of duties and allocated access rights are reviewed periodically.

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

### 3.7.1.2 Security configuration

Customers are responsible for ensuring that appropriate password requirements on their own systems and applications are implemented. Furthermore, it is the customers own responsibility to assess whether designing and implementing a security log control would be appropriate given the customers own control environment and the risks associated with the controls.

### 3.7.1.3 Business continuity management

Mentor IT has implemented procedures to support the recovery and restoration of the infrastructure and servers in the data centres. The customers should establish their own business continuity plans around their internal organisation and align them with the procedures performed by Mentor IT in case of an emergency to ensure that the operation of the customer's environment can be re-established according to the customer's expectations.

### 3.7.1.4 Compliance with relevant legislation

Mentor IT has planned procedures and controls in such a way that the legislation governing the areas for which Mentor IT is responsible is duly complied with. Mentor IT is not responsible for applications running on hosted equipment, and therefore this report does not extend to assuring that adequate controls have been established in the user applications and that the applications observe the Danish Bookkeeping Act, GDPR or other relevant legislation.

# 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. |
| *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 Overview of control objectives, control activity, tests and test results

**Control objective 4.4.1: Information security policies**

*To provide Management direction and support for information security in accordance with business requirements and relevant laws and regulations.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.1.1* | *IT policy*<br>Mentor IT has prepared an IT policy as a part of the employee handbook, which sums up security-related guidelines. The policy is issued by Management. | We have inspected the IT policy and verified that it contains IT security guidelines and is issued by Management. | No exceptions noted. |
| *4.4.1.2* | *Risk analysis*<br>Mentor IT has prepared an IT risk analysis that sums up the probability and consequences regarding the risks identified. The analysis has been approved by Management. | We have inspected the risk analysis and verified that the analysis had been approved by Management. | No exceptions noted. |

**Control objective 4.4.2: Access control**

*To ensure authorised user access and to prevent unauthorised access to systems and services.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.2.1* | *Passwords*<br>Security parameters regarding passwords on the management net have been set up using the standard Windows password setting. | We have inquired Management regarding the procedures/control activities performed. We have inspected systems and has assessed whether systems' settings comply with the baselines and security standards defined by Mentor IT. | No exceptions noted. |
| *4.4.2.2* | *Profiles*<br>All employees of Mentor IT are assigned individual and personal user profiles. All administrators have two individual profiles: One for regular use and one for administrative use. | We have inquired Management regarding the procedures/control activities performed We have inspected whether users have designated personal user accounts. Further, we have observed that individual administrator profiles are used. | No exceptions noted. |
| *4.4.2.3* | *User creation*<br>User administration procedures have been prepared, and all internal user creations are initiated by either HR or Management and are documented, either online or in manual folders. | We have inquired Management regarding the procedures/control activities performed. Based on a sample testing, we have inspected whether users were created according to the established procedure. | No exceptions noted. |
| *4.4.2.4* | *Administrative rights*<br>Only a few selected users have administrative rights to the Mentor IT domain. Administrator access rights are approved by Management according to the user administration procedure. All administrators use individual user profiles. | We have inquired Management regarding the procedures/control activities performed. We have inspected all users with administrative rights on the Mentor IT domain and verified them with Management. | No exceptions noted. |
| *4.4.2.5* | *User termination*<br>Users are terminated when they leave the company. Management prepares and approves the termination form, and based on this, system access is revoked. | We have inquired Management regarding the procedures/control activities performed assessed the procedures used and the controls performed. We have inspected a sample of users belonging to terminated employees and verified that the corresponding user profiles were disabled on the management network at Mentor IT. | No exceptions noted. |

**Control objective 4.4.2: Access control**

*To ensure authorised user access and to prevent unauthorised access to systems and services.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.2.6* | *Periodic review*<br>Users and their access rights for internal systems and client data are reviewed on a regular basis by Management. The review is performed according to an internal procedure and documented afterwards. | We have inquired Management regarding the procedures/control activities performed We have inspected documentation for user access rights reviews performed during the audit period and verified the results thereof. | No exceptions noted. |

**Control objective 4.4.3: Physical and environmental security**

*To prevent unauthorised physical access and damage to and interference in the organisation's information and information processing facilities.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.3.1* | *Access to critical locations*<br>An access control mechanism consisting of key card and a security code is installed for both Mentor IT's employees and customers with access to the data centres.<br>The security code is always required when entering the data centre through the external access ways. During opening hours, Mentor IT's employees can enter using their key card, only. | We have inquired Management regarding the procedures/control activities performed. We have inspected the list of people with access to the primary data centre as well as users granted access to Mentor IT's secondary site. | No exceptions noted. |
| *4.4.3.2* | *Environmental mechanisms*<br>The following environmental mechanisms are installed:<br>• Alternative power<br>• Fire detection/suppression<br>• Environmental monitors<br>• Cooling system.<br>All environmental security mechanisms are subject to regular maintenance service and testing. | We have inspected both the primary data centre and the secondary data centre to verify usage of adequate environmental mechanisms and has inspected the physical considerations. Furthermore, we have inspected the documentation regarding internal testing of the environmental mechanisms and the latest service reports. | No exceptions noted. |

**Control objective 4.4.4: Operations security**

*To protect against loss of data.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.4.1* | *Backup strategy*<br>The back-up strategy and selections are discussed individually with each client and aligned with customer expectations. | We have inquired Management regarding the procedures/control activities performed. We have inspected documentation for the image backup configuration and tested, for a sample of customers, that image backup was configured according to the agreements. | No exceptions noted. |
| *4.4.4.2* | *Backup storage*<br>Backup data is stored at the secondary data centre. | We have inquired Management regarding the procedures/control activities performed. We have inspected that image backup data in general was transferred to the off-site location.<br>We have inspected the primary and the secondary data centre to ensure that the backup storage location is appropriate. | No exceptions noted. |
| *4.4.4.3* | *Restoration test of backup*<br>Restore test of backups is performed on a regular basis according to an internal procedure. The test is documented. | We have inquired Management regarding the procedures/control activities performed. Further, we have inspected the documentation for a sample of restoration tests from the image backup. | No exceptions noted. |
| *4.4.4.4* | *Backup monitoring*<br>On a daily basis, the backup administrator reviews the relevant backup reports generated by the backup clients. If any irregularities occur, they will be handled. | We have inquired Management regarding the procedures/control activities performed. We have inspected the backup monitoring control and tested for a sample during the audit period whether irregularities are handled and documented. | No exceptions noted. |

**Control objective 4.4.5: Operations**

*To record events and generate evidence.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.5.1* | *Written guidelines and procedures*<br>Mentor IT has written standard operating procedures regarding the controls and procedures performed in connection with the provision of the agreed-upon services. | We have inquired Management regarding the procedures/control activities performed. We have inspected that written standard operating procedures are stored on the intranet and are available topersonnel with work related need. | No exceptions noted. |
| *4.4.5.2* | *Logs*<br>Access to the internal management net at Mentor IT and access to Remote Desktop (client data) are logged and stored. In case of security violations, unauthorised attempts to access information resources, e.g., reports, can be generated from the logs. | We have inquired Management regarding the procedures/control activities performed. We have inspected the log settings set on the internal management net and Remote Desktop.<br>We have inspected a log sample to verify that logging was performed throughout the audit period. | No exceptions noted. |

**Control objective 4.4.6: Change management – Network**

*To ensure protection of information in networks and its supporting information processing facilities.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.6.1* | *Patch management*<br>Patching of network equipment is performed based on an assessment of the relevant firmware/software. Network firmware is only installed if any critical security issues are discovered and if there is a high risk of exploitation. | We have inquired Management regarding the procedures/control activities performed. We have inspected the procedures for change management for network equipment.<br>We have inspected, on a sample basis, whether core network equipment has been patched according to the procedure.<br>We have inspected, by sample testing, that network devices have been updated by critical patches based on approved procedures. . | No exceptions noted. |
| *4.4.6.2* | *Fallback*<br>No specific fallback controls are performed. The core network is redundant, and a failover mechanism is in place. Network firmware is only installed if any critical security issues are discovered and if there is a high risk of exploitation. Backup copies are regularly made of all network configurations. | We have inquired Management regarding the procedures/control activities performed. We have inspected the procedures regarding fallback when changes to network and communication software are performed. | No exceptions noted. |
| *4.4.6.3* | *Documentation*<br>All major changes to network in the datacenter are documented. Network changes are recorded for internal use. | We have inquired Management regarding the procedures/control activities performed. We have inspected Mentor IT's controls on ensuring that network documentation is up to date to reflect the present environment.<br>We have inspected, on a sample basis, whether major network changes are documented. | No exceptions noted. |

**Control objective 4.4.7: Change management – Servers**

*To ensure that productive information systems are updated and secure according to Management's expectations.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.7.1* | *Patch management*<br>Systems software is regularly updated according to the customer agreements, usually each month. The update frequency is based on the content of the updates delivered by Microsoft and the approval from customers. | We have inquired Management regarding the procedures/control activities performed. We have inspected the patch management standards and observed that the procedure for patch management is being followed as described.<br>For a sample of patches, we have inspected that they were implemented on customers' and internal servers. | No exceptions noted. |
| *4.4.7.2* | *Documentation*<br>The customers' systems are documented in a host contract.<br>The customers' assets are collected automatically within the vendor's asset management system, supported by manual entries of assets when applicable, ensuring comprehensive asset coverage for the customers. | We have inquired Management regarding the procedures/control activities performed. We have observed that systems software documentation was up to date to reflect the present environment.<br>We have inquired Management regarding the procedures/control activities performed. We have inspected, for a sample of customers, that up-to-date systems documentation was available. | No exceptions noted. |

**Control objective 4.4.7: Problem and incident management**

*To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.8.1* | *Problem management*<br>Automated monitoring is established on all servers and services, and automatic alerts to operations staff are established. Usually, the alarms include the standard infrastructure components as hard-disc space running low, extended response time on networks, etc. In addition, all alerts are recorded. | We have inquired Management regarding the procedures/control activities performed. . We have inspected on a sample basis, that standard monitoring of infrastructure components has been set up, and that alerts were handled. | No exceptions noted. |
| *4.4.8.2* | *Incident management*<br>All customer requests are handled through the incident management system in which customers can report incidents to the support team, which documents actions performed to complete the client request. | We have inquired Management regarding the procedures/control activities performed. assessed the procedures and checks performed. We have examined samples of incidents and verified that actions performed are documented in the incident system. | No exceptions noted. |

**Control objective 4.4.9: Information security aspects of business continuity management**

*Information security continuity shall be embedded in the organisation's business continuity management systems.*

| No. | Service organisation's control activity | Tests performed by PwC | Result of PwC's tests |
|---|---|---|---|
| *4.4.9.1* | *Planning*<br>Mentor IT has prepared a disaster recovery plan, which has been approved by Management. The plan supports the restoration and recovery of the infrastructure supporting the customers' environments. | We have inquired Management regarding the procedures/control activities performed. We have inspected the disaster recovery plan and noted that it's content in terms of Mentor IT's internal organisation and procedures used. | No exceptions noted. |
| *4.4.9.2* | *Test*<br>The disaster recovery plan is tested periodically – but at least every second year (desktop test) by the responsible team and Management, and the results have been formally documented. | We have inquired Management regarding the procedures/control activities performed. We have inspected the documentation describing the internal desktop test of the disaster recovery plan. | No exceptions noted. |

PENN3O

*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."*

**Søren Frandsen**
**Kunde**
*Serienummer: f21df1bd-75d7-4e24-b2f3-84cef029c8a6*
*IP: 93.160.xxx.xxx*
*2024-04-19 17:20:10 UTC*

**Jesper Parsberg Madsen**
**PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231**
**Statsautoriseret revisor**
*Serienummer: 1845f1c8-669f-42ab-ba7e-8a1f6ea3011e*
*IP: 87.49.xxx.xxx*
*2024-04-19 18:01:04 UTC*

**Iraj Bastar**
**PRICEWATERHOUSECOOPERS STATSAUTORISERET REVISIONSPARTNERSELSKAB CVR: 33771231**
**PwC-medunderskriver**
*Serienummer: 945792b8-522b-4f8c-9f2d-bc89647c3d96*
*IP: 80.208.xxx.xxx*
*2024-04-19 18:01:10 UTC*

*Penneo dokumentnøgle: 6MXVU-T6I8X-KVOCO-GAF3M-J8EAA-GUSID*