Deloitte.

Deloitte
Statsautoriseret Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
P.O. Box 1600
0900 Copenhagen C
Denmark
Phone +45 36 10 20 30
Fax +45 36 10 20 40
www.deloitte.dk

Mentor IT A/S

ISAE 3402 Type 2

Independent auditor's report on general IT controls regarding operating and hosting services from 01.04.2016 to 31.03.2017

Contents

1. Independent auditor's report

To the management of Mentor IT A/S, Mentor IT A/S' customers and their auditors

Scope

We have been engaged to report on Mentor IT A/S' assertions in section 2 and the related descriptions of the system and control environment in section 3 with respect to Mentor IT A/S' operating and hosting services, comprising design, implementation, and effectiveness of controls as stated in the description. Mentor IT A/S' description refers to the controls established to ensure the system's security, data protection and operating efficiency of applications and the underlying infrastructure of the services, which Mentor IT A/S offers operating and hosting customers (general IT controls).

For further description of offered services, we refer to section 3.

This report is provided under the carve-out method and it does not comprise controls performed by subservice provider GlobalConnect. Services provided by GlobalConnect relate to physical security for the secondary backup site in Kolding.

Mentor IT A/S' responsibilities

Mentor IT A/S is responsible for preparing the accompanying assertions and the description of the system and control environment in section 3. Mentor IT A/S is also responsible for ensuring the completeness and accuracy of the description, including a correct representation and presentation of such assertion and description. Mentor IT A/S is also responsible for providing the services covered by the description and for designing and implementing effective controls to achieve the identified control objectives.

Information provided by Mentor IT A/S' management within section 5 of this report is not part of the system and control description provided, related to the services delivered to the clients, and has thus not been part of our audit or subject to our audit procedures performed.

Auditor's responsibilities

Based on our procedures, our responsibility is to express an opinion on Mentor IT A/S' description as well as on the design, implementation and effectiveness of controls related to the control objectives stated in this description. We conducted our engagement in accordance with the International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization", issued by the International Auditing and Assurance Standards Board. This standard requires that we comply with ethical requirements and that we plan and perform our procedures to obtain reasonable assurance that the description gives a fair presentation in all material respects and that the controls have been appropriately designed and that they are operating effectively.

We have complied with the requirements for independence and other ethical requirements in the IESBA's Code of Ethics, which is based on the fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional conduct.

Deloitte uses ISQC 1 and therefore maintains a comprehensive system for quality management, including documented policies and procedures for compliance with the code of ethics, professional standards, and applicable requirements according to the law and other regulations.

An assurance engagement relating to the description, design, and effectiveness of controls at Mentor IT A/S includes performing procedures to obtain evidence about Mentor IT A/S' description of its system and about the design and effectiveness of the controls. The procedures selected depend on the auditor's judgment, including judgment of the risk that the description is not presented fairly and that controls have not been suitably designed or that they are not functioning effectively. Our procedures include testing of the effectiveness of the controls we consider necessary to provide reasonable assurance that the control objectives stated in the description have been achieved. Our procedures also include evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service provider and described in section 2.

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

Limitations of controls at a service organization

Mentor IT A/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 control of a system that each individual customer may consider important in their own particular control environment. Also, because of their nature, controls at a service organization may not prevent or detect all errors or omissions in processing or reporting transactions. Moreover, the change in the assessment of effectiveness is subject to the risk that controls in a service organization may become insufficient or may fail.

Furthermore, using our opinion on subsequent periods' transactions will be subject to a risk that changes may have occurred in systems or controls or in the service organization's compliance with the policies and procedures described, which may cause that our opinion is no longer applicable.

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 2. It is our opinion that:

a) The description of the general IT controls fairly presents Mentor IT A/S' services of relevance to the system's security, data protection and operating efficiency for Mentor IT A/S' customers such as designed and implemented in the period from 01.04.2016 to 31.03.2017 in all material respects

b) The controls related to the control objectives stated in the description were suitably designed in the entire period from 01.04.2016 to 31.03.2017 in all material respects

c) The tested controls, which were the controls necessary to provide reasonable assurance that the control objectives in the description were achieved in all material respects, have functioned effectively in the entire period from 01.04.2016 to 31.03.2017.

Description of tested controls

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

Intended users and purpose

This report, the description of the system and control environment in section 3, and our tests of controls in section 4 are intended only for customers, who have used Mentor IT A/S' services, and their auditors who have a sufficient understanding to consider it along with other information, including information about the customers' own controls when identifying the risk of material misstatement of their financial statements.

Copenhagen, June 1, 2017

Deloitte

Statsautoriseret Revisionspartnerselskab

M. Bagger

Thomas Kühn
Partner, State Authorized Public Accountant

Michael Bagger
Senior Manager, CISA

2. Assertions by Mentor IT A/S

This report is prepared for Mentor IT A/S' customers using Mentor IT A/S' services and their auditors. Our statement includes the description of the system and control environment, including controls that Mentor IT A/S performs for customers in relation to the contracts with Mentor IT A/S. Our description of the processes and the controls carried out are described in Section 3 - System Description from Mentor IT A/S.

Our description covers the period from 01.04.2016 to 31.03.2017 and requires that customers and their auditors have sufficient understanding of and about the services provided to assess the description along with other information, including information about controls that customers have established and the assessment of risks of misstatement in customer accounts.

Mentor IT A/S confirms that:

1. The accompanying description in section 3 presents a fair description of the general controls related to Mentor IT's outsourcing services used by customers in the period from 01.04.2016 to 31.03.2017. The criteria for this assertion were that the included description:
    a. presents how the general IT controls were designed and implemented, including:
        i. the types of services provided, including, as appropriate, classes of transactions processed;
        ii. the processes in both IT and manual systems used for the management of the general IT controls;
        iii. relevant control objectives and controls designed to achieve these objectives;
        iv. controls which we, in regard to the controls' design, have assumed would be implemented by Mentor IT's customers, and which, if necessary in order to achieve the control objectives stated in the description, are identified in the description together with the specific control objectives, which we cannot achieve ourselves;
        v. other aspects of our control environment, risk assessment process, information system and communication, control activities and monitoring controls that have been relevant for the general IT controls.
    b. contains relevant information about changes in the general IT controls carried out during the period from 01.04.2016 to 31.03.2017.
    c. does not omit or distort information relevant to the scope of the described system, taking into account that the description is prepared to meet the common needs of a broad range of customers and their auditors and therefore cannot include any aspect of con-

trols, which each customer may deem important due to the customer's special conditions.

2. The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 01.04.2016 to 31.03.2017. The criteria for this assertion were that:
   a) the risks that threatened the achievement of the control objectives stated in the description were identified;
   b) the identified controls would, if applied as described, provide a high degree of assurance that those risks did not prevent the achievement of the stated control objectives, and that;
   c) the controls were applied consistently as designed, including that manual controls were carried out by persons with adequate competencies and authority throughout the entire period from 01.04.2016 to 31.03.2017.

Esbjerg, June 1, 2017
Mentor IT A/S

Søren Frandsen
Partner

3. Mentor IT A/S' system description

3.1 Overview

The purpose of this description is to inform customers of Mentor IT A/S and their auditors about the systems at Mentor IT and to ensure that the requirements of ”International Standard on Assurance Engagements 3402” and “Assurance Reports on Controls at a Service Organization” have been met. The description has also been made to inform about the controls in use to secure a safe and stable operation of the Hosting services (HS), Rack Hosting services (RS), and Support services (SS) delivered to Mentor IT A/S's customers.

This statement is an ISAE 3402 Type 2 statement, comprising a review of design, implementation and effectiveness of the controls at Mentor IT.

3.2 Mentor IT A/S and description of services

Mentor IT was founded in 1999 and their headquarters are located in Esbjerg, Denmark. Mentor IT is specialized in offering hosted solutions and managed services to companies. These services include server solutions, backup solutions, mail solutions, web hotels, CMS systems, online payment solutions and service desk solutions.

The facilities include two secure datacenters in Esbjerg. Both datacenters are owned by Mentor IT, and they are located more than five km from each other and connected through redundant fiber optics. All server systems are placed in Denmark, and redundant fiber connections from TDC, GlobalConnect and Stofa with very high bandwidth ensure that customers are provided with a quick and reliable solution. As of the end of June 2016, Mentor IT has moved their secondary datacenter from GlobalConnect's site in Kolding, to an internally managed second site in Esbjerg.

Mentor IT is a respected and well-established company within the hosting business. The offered services are based on world leading products and ”best practices” in order to ensure the customers the best possible solution and that they are not technologically bound to Mentor IT. The services and solutions are to be found on the company website, including current prices.

Mentor IT focuses on high quality and secure solutions, which a membership of and a quality certificate from the Danish Hosting Association (BFIH) confirms.

The solutions from 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

In the following, the controls in use regarding the Hosting Services (HS), Rack Hosting Services (RS), and Support Services (SS) delivered by Mentor IT are described. The services from Mentor IT are referred to as Mentor IT, which covers HS, RS, and SS. The services delivered by Mentor IT are described focusing on the established controls relevant for the ERP system platforms of Mentor IT A/S' customers.

The extent of the description is to include most of the customers at 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 centers.

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

- Hosting services (HS), including services such as:
  - Web hotel and DNS hotel
  - Mail scanning
  - Backup
  - Hosted Exchange
  - Hosted Desktop
  - Hosted Server
  - 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 agreement.

3.2.1.1 Hosting services (HS)

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

- Mentor IT A/S delivers the software for the operating systems. All data and configurations are backed up according to the customers' choices specified in their contracts. Service Level Agreements exist.
- For the individual customer systems, the customers are allowed to bring third-party software. Mentor IT must approve the software before installation.
- The systems are operated on a common hardware platform, where customers can choose between different levels of redundancy and functionality.
- Mentor IT is responsible for all administration and control of the hardware platform. The level of support and access to the systems follow the contract and SLA.

3.2.1.2 Rack Hosting (RH)

Customers with a request or demand for operating their own hardware platform are able to use Mentor IT's Rack Hosting Services, where they "rent" 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 are managed by Mentor IT
- Infrastructure can be supplied by Mentor IT, but customers are allowed to bring their own fiber connection.

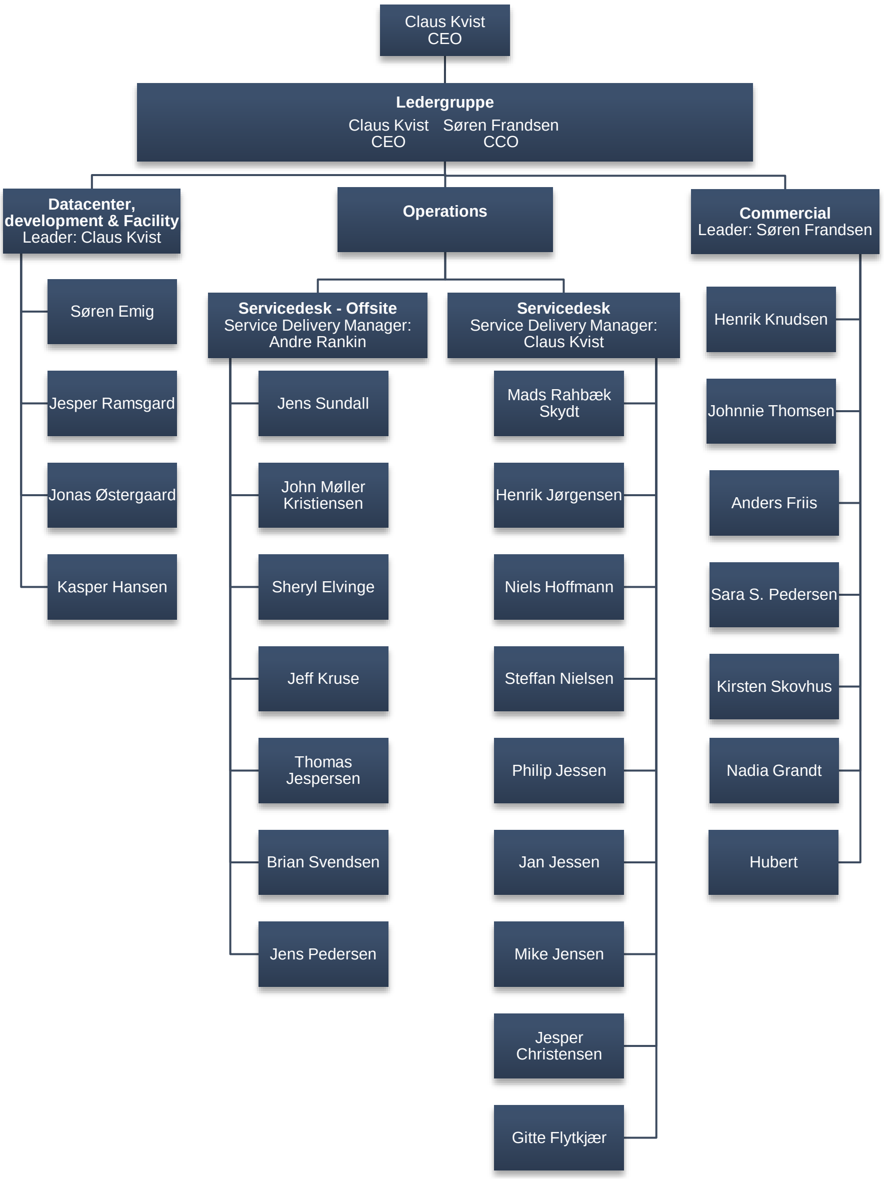
3.2.1.3 Support Services (SS)

Support Services are offered as an add-on to the customer's solutions and can be used as an alternative to the customer's own IT department, if such department does not exist, or if the customer sees it as financially attractive. The Support Services can be maintained on the customer's solution, where patches are installed and regular maintenance work is carried out. Support Service can also include user support on applications specified in the support contract. Furthermore, these services can be bought on an hour-to-hour basis for new projects, installation of new software, changing 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, which is specified in the contract.

- 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' organization and security

The organizational chart below shows the organization and responsibilities of Mentor IT A/S.



3.4 Risk assessment

The management of Mentor IT is responsible for identifying the risks and for establishing the required level of control to avoid these risks. This includes controls on the systems, facilities and infrastructure in the data centers of Mentor IT in Esbjerg.

Management meets 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 to identify potential risks.

On a yearly basis, the control team carries out a risk assessment on 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 have been used to produce the description of systems at Mentor IT. The same principles have also been used to assess whether the controls have been developed in a suitable way, and whether the controls are implemented in the organization.

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

The determination of criteria for control implementation at Mentor IT is based on ISO27001/27002:2013. Based on this control framework and on best practice, control areas and control activities have been implemented to minimize the risk of services provided by Mentor IT. Based on the control model chosen, the following control areas are included in the overall control environment:

- Information security policies
- Organization 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 Established control environment

Each area is described in detail in the following sections.

3.6.1 Information security policies

A formal IT security 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 and presented to all the employees to ensure that everyone understands and complies with it.

3.6.2 Organization 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 put on controls in politics, procedures, methods, and organizational 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 meet at least once each 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 result of Mentor IT
- Reports from auditors regarding financial and IT security
- The observations and recommendations of the control team.

3.6.2.2 Authorities

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

3.6.2.3 Control team

A control team has been established at Mentor IT. The team consists of specialists in finance, operational systems and the Standard Operation Procedure program. The control team has unlimited access to review the business of Mentor IT in order to ensure compliance with procedures. The control team reports directly to the management of Mentor IT.

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

- The internal controls regarding financial and legal obligations
- The internal controls regarding operational systems of the data centers
- The internal controls regarding procedures.

The control team will contribute to a 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 organizationally and functionally.

Procedures are in place to ensure that only the customers' management is able to order or confirm changes to services and user rights. The same management must also approve third-party suppliers to their services.

3.6.3 Human resources security

The recruitment procedures of Mentor IT have been standardized. When recruitment is required, Human Resources posts the available position, including a description of the tasks and responsibilities of the position. The candidates are reviewed regarding qualifications, and interviews are made. Whether a job offer is made depends on qualifications, references, personality, and criminal record.

The policies and procedures of Human Resources are available on the intranet of Mentor IT.

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 company intranet. The employees are to create value for the customers, be responsible, react to issues, communicate in an understandable way and be committed to their job.

All new employees in Mentor IT are required to participate in an introduction program. This program informs on the general policies, procedures and organization of Mentor IT and allows new employees to become familiar with the business philosophy.

Mentor IT has implemented various ways of communication to help its employees understand their individual roles and responsibilities, controls, and to help them ensure that important incidents are communicated in time. These include:

- Guidance programs 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.
- Newsletters and memos inform of important incidents and changes to company policies, and they are published regularly. Urgent information is communicated to the employees via email.
- Staff meetings are held twice a month or when necessary. These meetings offer the employees the opportunity to ask questions about the standard policies or exceptions to these.

All employees are entitled to vacation as specified in their contract of employment. The vacation must be approved by the supervisor. Upon retirement and employee terminations, interviews are made and the properties of the company are collected. Standard procedures are in place regarding collection of company property, deactivation of access keys and logins.

Mentor IT has a policy regarding equal treatment for men and women, with which all employees must be familiar.

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

3.6.4 Asset management

The data centers of Mentor IT are operated according to a ‘Best-of-Breed’ policy by only using hardware, software, and middleware from leading manufactures on the market, for example HP, Cisco, 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
- Fiber switches
- Data center switches
- Software for virtualization
- UPS
- Monitoring system
- Diesel generator
- Fire extinguishing equipment.

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

- Specific software licenses that can only be delivered to customers as a service:
  - For these licenses, service provider agreements have been made between Mentor IT and the manufacturer
- Customer hardware in the Rackspace 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 the employees can access.

The server and 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 separated from each other.

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 server and infrastructure team is necessary if a password has been deactivated.

Management of Mentor IT carries out control of personnel access. User access is updated by the server and infrastructure team.

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

3.6.5.2 User access management

User IDs are set up according to a process, where management informs the server and infrastructure team of new employees, the systems to which access is needed, and level of access. The manager of the new employee defines the level of access, which is based on the job description. Control of access to HS systems is conducted by top management.

The employees of Mentor IT may need access to Mentor IT's customer systems for maintenance or support purposes. This is made possible through numerous levels of logical access control. Every level of safety is adapted to the system platform, application and/or data files.

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 polices when creating new users. The information is given in the document "User creation".

3.6.5.4 Controls required to be performed by customer

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

The below mentioned controls are regarded as the minimum level of controls that a customer is required to have in order to ensure the level of security specified in this document. The list is not a complete list, since this depends on the transactions of the customer:

- **Access control**: The customer is responsible for implementing and administering access control to ensure that it prevents unauthorized 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 review 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 operational systems.

- **Change Management**: The customer is responsible for specifying and recognizing the need for testing of new patches and the authorization of new patches in their environment.

3.6.6 Physical and Environmental security

3.6.6.1 Security – physical access

Mentor IT has formal policies and procedures in place concerning access control to facilities and data centers. 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 centers are secured by key cards, which are connected to a central alarm unit. Access to facilities is granted in connection with job responsibility and is administrated by management according to internal procedures.

3.6.6.3 Surveillance

The entrances to the data centers are equipped with alarms and video surveillance. Video activity is transferred to a central server and is kept on SAN. Security personnel examine activation of door alarms. Furthermore, all access to the data center is monitored so that controlled/authorized access is maintained. Regular controls are conducted to secure that the list of employees that are allowed access is updated. Technicians in need of access due to business errands will be escorted.

3.6.6.4 Physical safety measures

Physical safety measures and control systems are in place to secure the data centers of Mentor IT against the surroundings. These systems include:

- Climate control in the data centers - HVAC (Heating, Ventilating and Air Conditioning) systems are monitored by Mentor IT personnel 24 hours a day, 7 days a week (24-7). Alarms inform employees of conditions, which deviate predetermined temperatures or levels of humidity. The employees respond to alarms and rectify the situation if necessary.
- Heat and smoke detectors are placed in the ceiling and under the elevated floor. 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 in the event of a possibly failure of these systems, alarms are in place to notify Mentor IT before reaching critical levels. These alarms are tested each time the generator and UPS are tested.
- Power Supply and backup facilities are installed and maintained to ensure continuous supply of electricity in case of loss of power. 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 a proper closing down of the system if necessary. The data centers are also equipped with backup diesel generators, which can be used to protect the data centers and the facility from irregularities in electricity and aid in case of a major power supply problem. UPS 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 normal walking areas. Especially cables for IT equipment are placed under an elevated floor or in a circuit under the ceiling.

Equipment outside the building is protected by a fence and is also monitored by video cameras.
Hardware no longer in service is stored for a certain period before 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 to ensure 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 on a daily basis. The image-based backup is performed to SAN in datacenter 2. Furthermore, documentation of all Mentor IT systems are copied to a USB key attached to a server in Mentor IT. These files are also copied to datacenter 2.

All backup reports are sent to the backup team for monitoring according to the SOP.

3.6.7.4 Backup of customer environments

Based on the customer’s backup agreement, backup is conducted on a daily basis.

Backup protects the customer’s data or systems regarding integrity and security. The backup is conducted every night or on another scheduled point in time through an automated process. To reduce restore time and/or to have an extra copy of the backup data, customers have the option of storing data on an extra external location. The backup data centers are placed in Esbjerg.

Two types of backup are available:

- File backup
- Image based backup (Snapshot backup).

Using the product ”File backup”, backup of files, databases and system files are taken. When using this product alone, it is not possible to restore a server from the backup. A basic installation is required before data from the backup can be restored. The customer is allowed 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. The file-based backup is first stored at data center 1 to increase performance and reduce restore time. The backup data is then replicated to data center 2.

”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 taken. Normally a 21-day backup history is used, but this may vary. The customer is not allowed access to the backup product. Restoring files or systems is only available through the support team of Mentor IT. Customer specific requirements regarding backup history can be arranged. The image-based backup is stored at data center 2.

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

3.6.7.5 Monitoring

The customers' operational systems are installed with standard logging of system events, application events and user events. These logs are backed up according to the backup agreement between Mentor IT and the customer.

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 send notifications if predetermined parameters are deviated. These parameters are defined at a level, where the notification will arrive in time for the incident to be solved inside opening hours without escalating the incident. Another predetermined set of parameters will activate a warning when deviated. The warnings are dealt with according to the SOP.

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

If the customer requests additional monitoring, this can be added and is then dealt with under customer specific requirements according to the contract.

Other monitoring systems

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

Logging of errors

The primary monitoring systems log all notifications for one year. Errors related to physical hardware, i.e. disc failure, are logged according to the SOP.

Timeservers

Where possible, all services are configured to synchronize with standard time servers on the Internet.

3.6.7.6 Responsibilities

The management and delivery of Mentor IT services are carried out by several teams in Mentor IT as defined in the organization of Mentor IT in section 3.3.

Operation and maintenance team

The maintenance and support team is responsible for the daily activities regarding monitoring, planning, solving problems, 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 routines, and that any problems are traced, registered, and solved. Problems regarding operation are logged according to the SOP, so that recurring problems are easily identified. The SOP includes necessary precautions for restart of services and restoration of systems in case of application or server problems.

The maintenance and support team is also responsible for:

- Control of Backup and Restore.
- Maintenance of operating systems for customers with this option.
- Maintenance of all hardware in the data centers of Mentor IT, including repair and replacement. Equipment of customers using Rack Hosting Services is not included in the maintenance program.
- Securing a reasonable store of spare parts for all hardware used to deliver Mentor IT services.

Infrastructure team

The consultant team is responsible for creating, supporting and implementing a standardized, secure infrastructure to the customers using Mentor IT services, ensuring a stable and highly available solution.

Support team

The support team of Mentor IT offers first level support on all Mentor IT services. The consultant team offers second level support. Support is offered when incidents are reported by phone or email. The support includes investigation of and solution to technical and system related incidents. All incidents are logged in the CRM system or ERP system depending on the incident. Support is 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 possibility to receive support outside 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, since it depends on the incident and the customer's contract.

Facility team

The maintenance and support team of Mentor IT is responsible for controlling all the data center facilities. Through close cooperation with management and the consultant team, it ensures that all activities are supported and that service contracts are in place for all relevant equipment.

3.6.7.7 Third party delivery management

The service level of suppliers is controlled on a regular basis. If deviations from contracts occur, the supplier will be contacted and the deviation corrected. If this is not possible, the supplier will be changed.

3.6.7.8 System planning and acceptance

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

When capacity usage is approaching 80%, management will be informed. All systems in Mentor IT are scalable, making purchase 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 fiber broadband in order to deliver cost-effective and scalable connections from the business location of the customers to the data centers of Mentor IT. Mentor IT collaborates with 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 fiber connections from one company fail. Only management and team leader from Mentor IT have access to the RIPE NCC services.

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

Internet & MPLS access is provided through redundant fiber solutions from multiple Internet Service Providers. These connections are physically separated until connected to the network. Combined with 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 customer's servers is specific to the customer's employees and the support team of Mentor IT.

Customers are able to buy service and maintenance on 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 centers is reviewed on a regular basis to ensure that the customers' needs and requirements are fulfilled.

3.6.9 Systems aquisition, development and maintenance

New hardware or systems to Mentor IT is discussed and tested by a relevant technical team before being approved by management.

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

Major changes to hardware or systems of Mentor IT require approval of management in accordance with the SOP. A change request process is applied for all major changes to software and hardware.

3.6.9.1 Patch management

On service agreements - where the customer has signed an agreement with Mentor IT on "preventive maintenance" (Forebyggende vedligehold) – Mentor IT will perform patch management on behalf of the customer. This service is defined as a service from Mentor IT where relevant patches, evaluated by employees of Mentor IT, are installed on operating systems and MS Office products on the customer's servers. Furthermore, logs from the operation system are evaluated.

Mentor IT monitors the update status of the servers according to the time defined in the agreement. Customers will - based on recommendations from Mentor IT - decide when the updates are to be implemented. Mentor IT is responsible for implementing updates in accordance with the customer's instructions. The time of the update process is agreed upon with the customer.

Patching of network equipment is done based on evaluation of the relevant firmware/software. The infrastructure team at Mentor IT monitors releases of firmware for the network equipment and applies relevant updates.

3.6.9.2 Protection against cyber-crime

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 possibilities 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 the incidents from happening 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 corporation 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 management except for major incidents. They all require a detailed written report from the relevant team.

Mentor IT has implemented several methods of communication to ensure that the customers understand the roles and responsibilities of Mentor IT, and in order 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 all evaluated, and root causes must be identified. Based on the incident and root cause, management and the technical team decide on changes to avoid the reoccurrence of such incident in the future.

3.6.11 Information security aspects of business continuty 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 centers in Esbjerg or establish operation elsewhere. It also includes checklists, contact lists, and procedures in order to ensure the contingency of Mentor IT.

The contingency plan is tested every second year with participation of all employees and management. The control team is responsible for setting up a "scenario" that challenges the participants.

Findings and improvements are discussed with management and the contingency plan is updated.

3.7 Additional information on the control environment

3.7.1 Matters to be considered by the customers’ auditors

3.7.1.1 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 comprised by this report. The customers’ own auditors should therefore assess whether this report can be extended to the specific customer and they should identify any other risks that are found material for the presentation of the customers’ financial statements.

3.7.1.2 User administration

Mentor IT grants access and rights in accordance with customer instructions. Mentor IT is not responsible for this information being correct, and it is thus the customers’ responsibility to ensure that the access and rights to the systems and applications are provided adequately and in compliance with best practice relating to segregation of duties.

Mentor IT also provides access to third party consultants, primarily developers, who are to maintain applications, which are part of the hosting agreement. This is made according to instructions from Mentor IT’s customers.

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

3.7.1.3 Compliance with relevant legislation

Mentor IT has planned procedures and controls in such a way that legislation in the areas for which Mentor IT is responsible is adequately observed. Mentor IT is not responsible for applications run on hosted equipment, and consequently, this report does not extend to assure that adequate controls have been established in the user applications and that the applications observe the Danish Bookkeeping Act, the Danish Act on Processing of Personal Data, or other relevant legislation.

4. Information provided by Deloitte

4.1 Introduction

This outline has been prepared in order to inform customers of controls performed by Mentor IT A/S that may affect the treatment of accounting transactions and to state the effectiveness of the controls checked by us. This section, combined with an understanding and assessment of the controls involved in the customers’ business processes, aims to assist the customers' auditors to plan the audit of the financial statements and to assess the risk of misstatements in the customers’ financial statements that may be affected by controls performed by Mentor IT A/S.

Our testing of Mentor IT A/S’ controls is limited to the control objectives and related controls referred to in the test table below and is not extended to include all of the controls described in management’s description of the system. In addition, controls performed at the premises of Mentor IT A/S’ customers are not covered by our report. It is assumed that the latter controls are examined and assessed by the customers’ own auditors.

This report is provided under the carve-out method and it does not comprise controls performed by subservice provider GlobalConnect. Services provided by GlobalConnect relate to physical security for the secondary backup site in Kolding.

Finally, the customers may have established compensating controls that help to minimize the control weaknesses referred to in this report to a level acceptable for audit purposes. Such assessment can only be made by the customers’ auditors.

4.2 Control environment elements

Our testing of the control environment involved interviewing relevant members of management, supervisors and employees as well as examining Mentor IT A/S’ documents and recordings. The control environment has been assessed in order to determine the nature, timing, and scope of the effectiveness of controls.

4.3 Test of effectiveness

Our test of the effectiveness of controls includes the tests we consider necessary to evaluate whether the controls performed and the observance of these controls are sufficient to provide a firm, but not an absolute, conviction that the control objectives specified have been achieved in the period from 01.04.2016 to 31.03.2017. Our test of the effectiveness of controls is designed to cover a representative number of transactions during the period from 01.04.2016 to 31.03.2017 for any control designed to achieve the specific control objective. See below for details. When selecting specific tests, we considered

(a) the nature of the areas tested, (b) the types of available documentation, (c) the nature of audit objectives to be achieved, (d) the assessed control risk level, and (e) the estimated effectiveness of the test.

4.4 Control objectives and control activities

The table below states the control objectives and controls tested. It also states the audit procedures performed and the results thereof along with any material control weaknesses we may have identified.

4.4.1 Information security policies

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.			
4.4.1.1 *Security policy*	Mentor IT has prepared an IT security policy, which sums up security related issues. The policy has been approved by management.	Deloitte has reviewed the security policy and verified that the policy has been approved by management.	No deviations noted
4.4.1.2 *Risk analysis*	Mentor IT has prepared an IT risk analysis that sums up the probability and consequences regarding the identified risks. The analysis has been approved by management.	Deloitte has reviewed the risk analysis and verified that the analysis has been approved by management.	No deviations noted.

4.4.2 Organization of information security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To establish a management framework that will initiate and control the implementation and operation of information security within the organization.			
4.4.2.1 *Organization*	Management at Mentor IT has defined roles and responsibilities in both Standard Operational Procedures and organizational diagrams.	Based on interviews and documentation, Deloitte has assessed whether roles are properly defined within the organization.	No deviations noted.

4.4.3 Access control

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
4.4.3.1 *Passwords*	Security parameters regarding passwords on the management net have been set up using the standard Windows password setting.	Deloitte has assessed the procedures used and the controls performed. Deloitte has performed a review of systems and has assessed whether systems comply with the baselines and security standards defined by Mentor IT. Based on the system security assessment, we have checked that parameters are enabled and are properly set up.	No deviations noted.
4.4.3.2 *Profiles*	All employees at Mentor IT are assigned individual and personal user profiles. All administrators have two individual profiles: One for regular use and one for administrative use.	Deloitte has assessed the procedures used and the controls performed. Based on our technical review of the Mentor IT domain, we have reviewed whether users have designated personal user accounts.	No deviations noted.
4.4.3.3 *Open network*	No open networks are used at Mentor IT. All traffic to clients is directed through secure connections, using DMVPN.	Deloitte has assessed the procedures used and the controls performed. We have assessed whether the data transmitted between Mentor IT and their customers is properly protected.	No deviations noted.
4.4.3.4 *User creation*	User administration procedures have been prepared and all internal user creations have been formally approved by management and documented either online or in manual folders.	Deloitte has assessed the procedures used and the controls performed. Based on a sample, we have assessed whether users were created according to the established procedure.	No deviations noted.
4.4.3.5 *Administrative rights*	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.	Deloitte has assessed the procedures used and the controls performed. We have reviewed all users with administrative rights on the Mentor IT domain and verified these with management.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
4.4.3.6 *User termination*	Users are terminated when employees leave the company. Management prepares and approves the termination form, and based on this, system access is revoked by the support team.	Deloitte has assessed the procedures used and the controls performed. We have reviewed a sample of users belonging to terminated employees and verified that the corresponding user profiles have been disabled on the management network at Mentor IT.	No deviations noted.
4.4.3.7 *Periodic review*	Users and their access rights to internal systems and client data are reviewed on a regular basis by management. The review is performed according to an internal procedure, and is documented. The support team performs follow-up on user access actions from the review	Deloitte has assessed the user access rights review during the audit period.	No deviations noted.

4.4.4 Physical and environmental security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To prevent unauthorized physical access and damage to and interference in the organization's information and information processing facilities.			
4.4.4.1 *Access to critical locations*	An access control mechanism consisting of keycard and a security code is installed for both Mentor IT's employees and their customers with access to the data centers.	Deloitte has assessed the procedures used and the controls performed. We have assessed the access control mechanism and reviewed the list of people with access to the primary data center, as well as users granted access to Mentor ITs secondary site.	No deviations noted.
4.4.4.2 *Environmental mechanisms*	The following environmental mechanisms are installed: • Alternative power • Fire detection/suppression • Environmental monitors • Cooling All environmental security mechanisms are subject to regular maintenance service and test.	Deloitte has assessed the procedures used and the controls performed. We have inspected the primary data center to verify the usage of adequate environmental mechanisms and reviewed the physical considerations. Furthermore, we have assessed the documentation regarding internal testing of the environmental mechanisms and reviewed the latest service reports.	No deviations noted.

4.4.5 Operations security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To protect against loss of data.			
4.4.5.1 *Backup strategy*	Backup strategy and selections are discussed individually with each client and aligned with customer expectations.	Deloitte has assessed the procedures used and the controls performed. We have obtained documentation regarding the backup strategy for a selection of customers and verified the backup configuration.	No deviations noted.
4.4.5.2 *Backup identification*	All backup data is stored on hard drives. No physical identification possible.	Deloitte has assessed the procedures used and the controls performed. We have examined whether any backup is stored on any media, which should be labeled.	No deviations noted.
4.4.5.3 *Internal backup storage*	Backup data is stored on hard drives in the primary data center and is automatically transferred to the secondary data center.	Deloitte has assessed the procedures used and the controls performed. We have examined the primary data center to ensure that the backup storage location is appropriate.	No deviations noted.
4.4.5.4 *External backup storage*	Backup data is stored on hard drives in the primary data center and is automatically transferred to the secondary data center.	Deloitte has assessed the procedures used and the controls performed. We have examined whether backup data has been transferred to the off-site location.	No deviations noted.
4.4.5.5 *Restoration test of backup*	Restore test of backups is performed on a regular basis according to an internal procedure. The restore test is performed by the support team and the test is documented.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the documentation on a selection of restoration tests (or recovery tests) and verified the approval.	No deviations noted.
4.4.5.6 *Written guidelines & procedures*	Mentor IT has written Standard Operating Procedures regarding the controls and procedures performed in connection with the delivery of the agreed upon services.	Deloitte has reviewed the written Standard Operating Procedures to verify that proper documentation is stored correctly and is available to relevant personnel.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
4.4.5.7 *Job control*	On a daily basis, the backup administrator reviews the relevant backup reports generated by the backup clients. If any irregularities occur, these will be handled in cooperation with the individual clients.	Deloitte has assessed the procedures used and the controls performed. We have taken a sample of the backup monitoring control during the audit period and tested whether irregularities are handled and documented.	No deviations noted.
Control objective: To record events and generate evidence.			
4.4.5.8 *Logs*	Access to the internal management net at Mentor IT and access to Remote Desktop (client data) are logged and stored in case of security violation reports, unauthorized attempts to access information resources, etc. No regular review of security logs is performed.	Deloitte has assessed the log mechanisms and procedures regarding security logging in general.	We have noted that security logging in general has been configured on relevant systems. Furthermore, we have been informed that review of security logs is performed on a regular basis. The reviews performed are not documented.

4.4.6 Communications security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To ensure the protection of information in networks and its supporting information processing facilities.			
4.4.6.1 *Patch management*	A formal service agreement has been established with an external supplier regarding change management and maintenance of the network. All changes to the network is performed and documented by the external vendor.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the patch management standards and assessed whether the procedure for patch management is followed as described.	No deviations noted.
4.4.6.2 *Timing*	All network configuration files are copied before they are changed and stored in a secure folder at the Mentor IT management domain.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the implementation process and checked whether the procedures for putting changes into production are appropriately performed.	No deviations noted.
4.4.6.3 *Fallback*	No specific fallback controls are performed. The core network is redundant and 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 exploitations.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the procedures regarding fallback when changes to network and communication software are performed.	No deviations noted.
4.4.6.4 *Documentation*	All changes to the network are documented. Network documentation is recorded in multiple documents for both internal use and the customers' network configurations.	Deloitte has assessed the procedures used and the controls performed. We have assessed whether network documentation was updated to reflect the present environment.	No deviations noted.

4.4.7 Systems acquisition, development and maintenance

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems, which provide services over public networks.			
4.4.7.1 *Patch management*	System software is regularly updated according to the customer agreements. The update frequency is based on the content of the updates delivered by Microsoft and the approval from customers.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the patch management standards and assessed whether the procedure for patch management is followed as described.	We noted for a single server on a separate internal network that security patches had failed during installation.
4.4.7.2 *Timing*	If it is decided to update the systems' software, a service window is agreed upon with the customer. This is documented in emails.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the implementation process and checked whether the procedures for putting changes into production are appropriately performed.	No deviations noted.
4.4.7.3 *Fallback*	Patches are not implemented into client environments until these have been tested on internal servers. If errors should occur, patches will be removed.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the procedures regarding fallback when changes to system software are performed.	No deviations noted.
4.4.7.4 *Documentation*	The customers' systems are documented in a host contract and in a technical description of the customers' setup.	Deloitte has assessed the procedures used and the controls performed. We have assessed whether system software documentation was updated to reflect the present environment.	No deviations noted.

4.4.8 Information security incident Management

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.			
4.4.8.1 *Problem and incident management*	All customer requests are handled through the incident management system, where the support team documents actions performed to complete the client request. Automatic monitoring is established on all servers and services and automatic alerts to operations staff is established. In addition, all alerts are recorded as incidents.	Deloitte assessed the procedures and checks carried out. Deloitte has examined samples of incidents from clients and alarms from the operating environment and checked that follow-up procedures were performed.	No deviations noted.

4.4.9 Information security aspects of business continuity management

Control Activity	Client Control Activity	Audit Procedures Performed	Test Result
Control objective: Information security continuity shall be embedded in the organization's business continuity management systems.			
4.4.9.1 *Planning*	Mentor IT has prepared a disaster recovery plan, which has been approved by management.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the disaster recovery plan and assessed the content.	No deviations noted.
4.4.9.2 *Test*	The disaster recovery plan has been tested (desktop test) by the responsible team and management, and the result has been formally documented.	Deloitte has assessed the procedures used and the controls performed. We have reviewed the documentation describing the internal test of the disaster recovery plan.	No deviations noted.

5. Mentor IT A/S' management comments

5.1 Remediation of audit finding 4.4.5.8 related to audit log settings and review

Security logs are reviewed on a regular basis. An automated review process has been tested and implemented.

5.2 Remediation of audit finding 4.4.7.1 related to patch management

Security patches had failed on a single internal server. The server is operated on a closed network with no internet access. The risk of being compromised is rated very low. However, we have implemented automated patch management on this server to ensure correct patches are installed.