Deloitte
Statsautoriseret
Revisionspartnerselskab
CVR no. 33 96 35 56
Weidekampsgade 6
2300 Copenhagen S

Phone: +45 36102030
www.deloitte.dk

Mentor IT

ISAE 3402 Type 2 Independent Service Auditor's Report on general IT controls regarding operating and hosting services

Throughout the period from 1 April 2021 to 31 March 2022

Table of Contents

1. Independent Service Auditor's Report

Independent Service Auditor's Assurance Report on the Description of Controls, their Design and Operating Effectiveness

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' (hereafter referred to as Mentor IT) description of the system and control environment in section 3 (the description) with respect to Mentor IT's operating and hosting services throughout the period from 1 April 2021 to 31 March 2022 and on the design, implementation and effectiveness of controls as stated in the description.

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. The opinion does not include 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 assertion in section 2, Service Organisation's assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor's Independence and Quality Control

We have complied with the requirements for independence in the IESBA's Code of Ethics for Professional Accountants, 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 for Professional Accountants, professional standards, and applicable requirements according to the law and other regulations.

Service Auditor's Responsibilities

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

We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "*Assurance Reports on Controls at a Service Organization*," issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and 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 system, and the design and operating effectiveness of controls. The procedures selected depend on the service auditor's judgment, including the assessment of the 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 by the service organisation and described in section 2, Service Organisation's assertion.

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

Opinion

Our opinion has been formed on the basis of the matters outlined in this report. The criteria we used in forming our opinion are those described in section 2. In our opinion, in all material respects:

(a) The description of the general IT controls fairly presents Mentor IT's controls of relevance to the hosting and operating services to Mentor IT's customers as designed and implemented in the period from 1 April 2021 to 31 March 2022;
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period from 1 April 2021 to 31 March 2022; 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 2021 to 31 March 2022.

Description of Tests of Controls

The specific controls tested, and the nature, timing and results of those 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 customers themselves, when assessing the risks of material misstatements of customers' financial statements.

Copenhagen, 12 July 2022

Deloitte
Statsautoriseret Revisionspartnerselskab

Thomas Kühn
Partner, State-Authorised Public Accountant

Michael Bagger
Partner, CISA

2. Service Organisation's Assertion

Mentor IT's Assertion

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 customers themselves, when assessing the risks of material misstatements of customers' financial statements. Mentor IT confirms that:

a) The accompanying description in section 3 fairly presents the general controls related to Mentor IT's outsourcing services used by customers throughout the period from 1 April 2021 to 31 March 2022. The criteria used in making this assertion were that the accompanying description:

i. Presents how the system was designed and implemented, including:
   - The types of services provided, including, as appropriate, classes of transactions processed.
   - The procedures within both information technology and manual systems by which those transactions were initiated, recorded, processed, corrected as necessary and transferred to the reports prepared for customers
   - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for customers
   - How the system dealt with significant events and conditions other than transactions
   - Relevant control objectives and controls designed to achieve those objectives
   - The process for preparing reports for customers
   - Relevant control objectives and controls designed to achieve those objectives
   - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve the control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved by ourselves alone.
   - Other aspects of our control environment, risk assessment process, information system (including the related business processes) and communication, control activities, and monitoring controls that were relevant to processing and reporting customers' transactions.

ii. Includes relevant details of changes to the general IT controls during the period from 1 April 2021 to 31 March 2022.

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 April 2021 to 31 March 2022. The criteria used in making this assertion were that:

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

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

iii. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 April 2021 to 31 March 2022.

Esbjerg, 12 July 2022

Mentor IT A/S

Søren Frandsen

Søren Frandsen
Partner

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' customers.

3.2 Mentor IT A/S and description of services

Mentor IT was founded in 1999 and is located in Esbjerg, Kolding, Århus 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, mail solutions, web hotels, and service desk solutions.

The facilities include two secure datacentres in Esbjerg. Both datacentres 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' 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 datacentres.

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 datacentres 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 is 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.

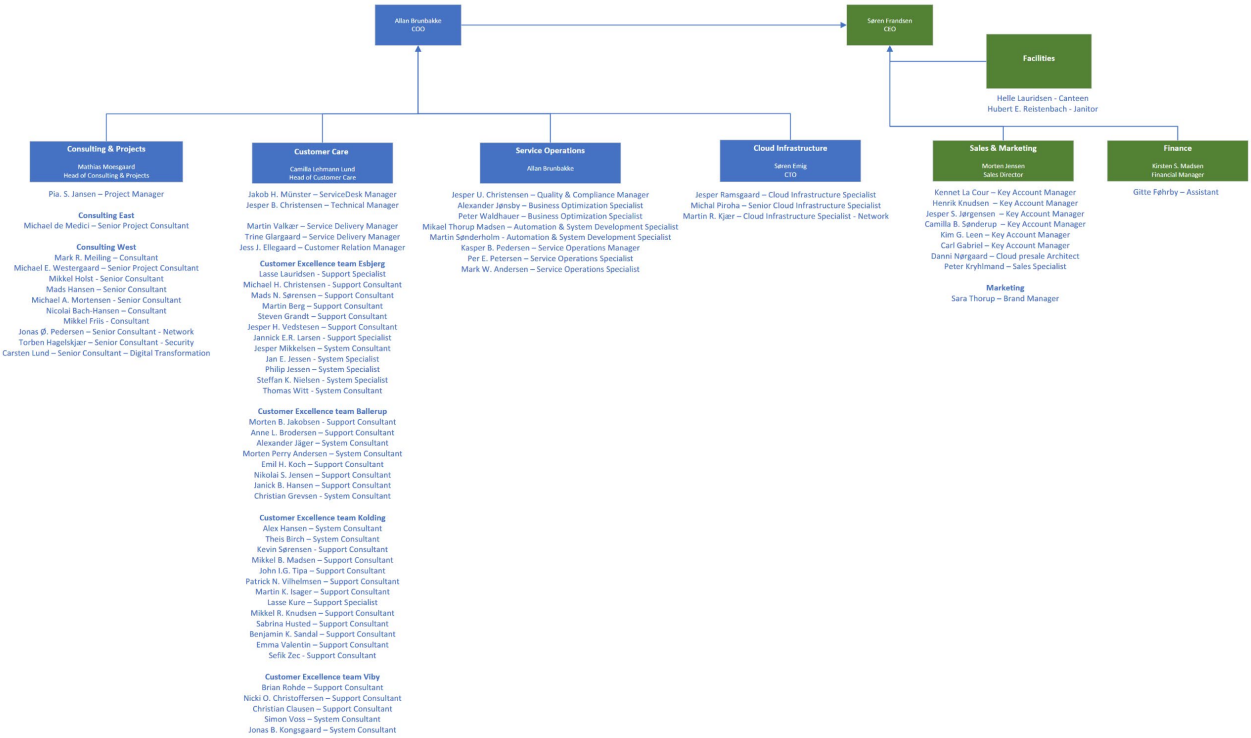
3.2.1.3 *Support Services (SS)*

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' organisation and security

The organisational chart below shows the organisation 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 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 ISO27001/27002:2013. 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 the 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 the 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 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 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 ensure that only the customers' management can 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 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 program. This program 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 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.
- 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 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 should be accessible by the employees. Access rights are preapproved based on three fixed user groups that reflect the group's work-related needs.

The Cloud infrastructure team are 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.

The management of Mentor IT 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 IDs are set up according to a process, with management informing the Cloud infrastructure team of new employees, the systems to which access is needed and the level of access. The manager of the new employee defines the level of access based on the employee's job description. Checks of access to HS systems are conducted by the 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 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 the 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 the 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 the customer's back-up agreement, 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. To reduce restore time and/or to have an extra copy of the back-up data, customers have the option to store data on an additional external location. The back-up data centres are placed in Esbjerg.

Two types of backup are available:

- File backup;
- Office 365 backup
- Image-based backup (snapshot backup).

Using the product "File backup", back-up copies are made of selected files, databases and system files. 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 back-up client and is able to restore and select files for backup. Configuration of several back-up jobs with different histories is also an option. The file-based backup is first stored at data centre 1 to increase performance and reduce restore time. The back-up data is then replicated to data centre 2.

Office 365 backup backs up Mails, 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 back-up history is used, but this may vary. The customer is not granted access to the back-up product. Restoring files or systems is only possible through the support team of Mentor IT. Customer-specific requirements regarding back-up history can be arranged. The image-based backup is stored at data centre 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 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, the level of uptime and time passed since the latest systems update.

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. Errors related to physical hardware, i.e. disc failure, are logged 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. The SOP includes necessary precautions for the restart of services and restoration of systems in case of application or server problems.

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*

The service level of suppliers is checked 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 replaced.

3.6.7.9 *System planning and acceptance*

Formal information and reporting systems have been implemented to ensure that the 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 the 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 is 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 the management.

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

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

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 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 the management and logged according to the SOP. There are no formal requirements as to the form of the report to be presented to the 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 the 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. The customers' own auditors should therefore assess whether this report can be extended to the specific customer by assessing whether the services described in this report are included in the services delivered to their customers, and they should identify any other risks that are found material to the presentation of the customers' financial statements.

3.7.2 *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 datacentres

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.

3.7.3 *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.

3.7.4 *Business Continuity Management*

Mentor has implemented procedures to support the recovery and restoration of the infrastructure and servers in the datacentres. The customers should establish their own business continuity plans around their internal organisation and align them with the procedures performed by Mentor 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.

3.7.5 *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. Service Organisation's Control Objectives and Related Controls, and Deloitte's Tests of Controls and Results of Tests

4.1 Introduction

This report is intended to provide Mentor IT's customers with information about the controls at Mentor IT that may affect the processing of user organisations' transactions and also to provide Mentor IT's customers with information about the operating effectiveness of the controls that were tested.

This report, when combined with an understanding and assessment of the controls at user organisations, is intended to assist user auditors in (1) planning the audit of user organisations' financial statements and in (2) assessing control risk for assertions in user organisations' financial statements that may be affected by controls at Mentor IT.

Our testing of Mentor IT's controls was restricted to the control objectives and related controls listed in the matrices in this section of the report and was not extended to controls described in the system description but not included in the aforementioned matrices, or to controls that may be in effect at user organisations. It is each user auditor's responsibility to evaluate this information in relation to the controls in place at each user organisation. If certain complementary controls are not in place at user organisations, Mentor IT's controls may not compensate for such weaknesses.

4.2 Test of Controls

The test of controls performed consists of one or more of the following methods:

Method	Description
Inquiry	Interview, i.e., inquiry with selected personnel at Mentor IT
Observation	Observation of the execution of control
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of the control. This includes reading and evaluating reports and other documentation to assess whether specific controls are designed and implemented. Furthermore, it is assessed whether controls are monitored and supervised adequately and at appropriate intervals.
Re-performance of control	Repetition of the relevant control to verify that the control functions as intended

4.3 Test of Operating Effectiveness

Our test of the operating effectiveness of controls includes such tests as we consider necessary to evaluate whether those controls performed, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved throughout the period from 1 April 2021 to 31 March 2022.

Our test of the operating effectiveness of controls was designed to cover a representative number of transactions throughout the period from 1 April 2021 to 31 March 2022 for each of the controls listed in this section, which are designed to achieve the specific control objectives.

4.4 Control Objectives, Controls, and Test Results

4.4.1 Information security policies

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
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 *IT policy*	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.	Deloitte has reviewed the IT policy and verified that it contains IT security guidelines and is issued 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 risks identified. The analysis has been approved by the management.	Deloitte has reviewed the risk analysis and verified that the analysis had been approved by the management.	No deviations noted.

4.4.2 Access control

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
4.4.2.1 *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 set up properly.	No deviations noted.
4.4.2.2 *Profiles*	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.	Based on our technical review of the Mentor IT domain, Deloitte has reviewed whether users have designated personal user accounts. Further, we have verified that individual administrator profiles are used.	No deviations noted.
4.4.2.3 *User creation*	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.	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.
4.4.2.4 *Administrative rights*	Only a few selected users have administrative rights to the Mentor IT domain. Administrator access rights are approved by the management according to the user administration procedure. All administrators are using individual user profiles.	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 them with the management.	No deviations noted.
4.4.2.5 *User termination*	Users are terminated when they leave the company. The 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 were disabled on the management network at Mentor IT.	No deviations noted.
4.4.2.6 *Periodic review*	Users and their access rights for internal systems and client data are reviewed on a regular basis by the management. The review is performed according to an internal procedure and documented afterwards. The support team follows up on user access actions from the review.	Deloitte has inspected documentation for user access rights reviews performed during the audit period and verified the results thereof.	No deviations noted.

4.4.3 Physical and environmental security

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent unauthorised physical access and damage to and interference in the organisation's information and information processing facilities.			
4.4.3.1 *Access to critical locations*	An access control mechanism consisting of key card and a security code is installed for both Mentor IT's employees and their customers with access to the datacentres. The security code is always required entering the datacentre through the external access ways. During opening hours, Mentor IT's employees can enter using their key card only.	Deloitte has assessed the access control mechanism and reviewed the list of people with access to the primary datacentre, as well as users granted access to Mentor IT's secondary site.	No deviations noted.
4.4.3.2 *Environmental mechanisms*	The following environmental mechanisms are installed: • Alternative power; • Fire detection/suppression; • Environmental monitors; • Cooling system. All environmental security mechanisms are subject to regular maintenance service and testing.	Deloitte has inspected both the primary datacentre and the secondary datacentre to verify usage of adequate environmental mechanisms and has 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.

4.4.4 Operations security

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: To protect against loss of data.			
4.4.4.1 *Back-up strategy*	The back-up strategy and selections are discussed individually with each client and aligned with customer expectations.	Deloitte has obtained documentation for the image back-up configuration and tested, for a sample of customers, that image backup was configured according to the agreements.	No deviations noted.
4.4.4.2 *Back-up storage*	Back-up data is stored at the secondary datacentre.	Deloitte has examined whether image back-up data in general was transferred to the off-site location. Deloitte has examined the primary and the secondary datacentre to ensure that the back-up storage location is appropriate.	No deviations noted.
4.4.4.3 *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. Further, we have reviewed the documentation for a sample of restoration tests from the image back-up.	No deviations noted.
4.4.4.4 *Backup monitoring*	On a daily basis, the back-up administrator reviews the relevant back-up reports generated by the back-up clients. If any irregularities occur, they will be handled in cooperation with the individual clients.	Deloitte has reviewed the back-up monitoring control and tested for a sample during the audit period whether irregularities are handled and documented.	No deviations noted.

4.4.5 Operations

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: To record events and generate evidence.			
4.4.5.1 *Written guidelines and procedures*	Mentor IT has written Standard Operating Procedures regarding the controls and procedures performed in connection with the provision of the agreed-upon services.	Deloitte has verified that written Standard Operating Procedures are stored on the intranet and are available to relevant personnel.	No deviations noted.
4.4.5.2 *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 violations, unauthorised attempts to access information resources, e.g., reports, can be generated from the logs.	Deloitte has reviewed the log settings set on the internal management net and Remote Desktop. Deloitte has reviewed a log sample to verify that logging was performed throughout the audit period.	Deloitte has noted for 10 out of 15 sampled days, that logs were not obtained and stored from the Remote Desktop Manager. Deloitte has been informed that Mentor IT has resolved the issue and strengthened the control to avoid non-storage of log-files. No further deviations noted.

4.4.6 Change Management - Network

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure protection of information in networks and its supporting information processing facilities.			
4.4.6.1 *Patch management*	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.	Deloitte has reviewed the procedures for change management for network equipment. Deloitte has verified, on a sample basis, whether core network equipment has been patched according to the procedure. Deloitte has verified with key personnel at Mentor IT that no critical updates for network equipment, are pending.	No deviations noted.
4.4.6.2 *Fallback*	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. Back-up copies are regularly made of all network configurations.	Deloitte has reviewed the procedures regarding fallback when changes to network and communication software are performed.	No deviations noted.
4.4.6.3 *Documentation*	All major changes to the network are documented. Network changes are recorded for both internal use and for the customers' network configurations.	Deloitte has assessed the Mentor IT's controls on ensuring that network documentation is up to date to reflect the present environment. Deloitte has verified, on a sample basis, whether major network changes are documented.	No deviations noted.

4.4.7 Change Management - Servers

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that productive information systems are updated and secure according to management's expectations.			
4.4.7.1 *Patch management*	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.	Deloitte has reviewed the patch management standards and assessed whether the procedure for patch management is being followed as described. For a sample of patches Deloitte has tested that they were implemented on customers' and internal servers.	No deviations noted.
4.4.7.2 *Documentation*	The customers' systems are documented in a host contract and in a technical description of the customers' setup.	Deloitte has assessed whether systems software documentation was up to date to reflect the present environment. Deloitte has tested, for a sample of customers, that up-to-date systems documentation was available.	No deviations noted.

4.4.8 Problem and incident management

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
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 management*	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.	Deloitte has assessed the procedures and checks performed. Deloitte has examined on a sample basis that standard monitoring of infrastructure components has been set up, and that alerts were handled.	No deviations noted.
4.4.8.2 *Incident management*	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.	Deloitte has assessed the procedures and checks performed. Deloitte has examined samples of incidents and verified that actions performed are documented in the incident system.	No deviations noted.

4.4.9 Information security aspects of business continuity management

Control Activity	Mentor IT's Control Activity	Audit Procedures Performed	Test Results
Control objective: Information security continuity shall be embedded in the organisation's business continuity management systems.			
4.4.9.1 *Planning*	Mentor IT has prepared a disaster recovery plan, which has been approved by the management. The plan supports the restoration and recovery of the infrastructure supporting the customers' environments.	Deloitte has reviewed the disaster recovery plan and assessed its content in terms of Mentor's internal organisation and procedures used.	No deviations noted.
4.4.9.2 *Test*	The disaster recovery plan is tested periodically – but at least every second year (desktop test) by the responsible team and the management, and the results have been formally documented.	Deloitte has reviewed the documentation describing the internal desktop test of the disaster recovery plan.	No deviations noted.

5. Other Information Provided by Mentor IT Management's Response to Deviations Noted

4.4.5 Operations

Control Activity	Mentor IT's Control Activity	Deviations Noted	Management Response
Control objective: To record events and generate evidence.			
4.4.5.2 *Logs*	Access to the internal management net at Mentor IT and access to Remote Desktop (client data) is logged and stored. In case of security violations, unauthorised attempts to access information resources, e.g., reports, can be generated from the logs.	Deloitte has noted for 10 out of 15 sampled days that logs were not obtained and stored from the Remote Desktop Manager. Deloitte was informed that Mentor IT has resolved the issue and strengthened the control to avoid non-storage of logfiles. No further deviations noted.	Due to a bug in a software update, logs have not been collected for a period of time after a software update of the Remote Desktop Manager. This has been resolved. Furthermore, Mentor IT has implemented several measures to prevent this from happening again. Mentor IT has: - Included logs in the SIEM tool for central log management - Ensured manual control of the logs on a regular basis and documentation thereof.