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

TimePlan Software A/S

ISAE 3402 Type 1

Independent auditor’s report on general IT controls regarding support and development services as of 26 October 2018

Contents

1. Independent auditor’s report

To the management of TimePlan Software A/S, TimePlan Software A/S’s customers and their auditors

Scope

We have been engaged to report on TimePlan Software A/S’s assertion in section 2 and the related descriptions of the system and control environment in section 3 with respect to TimePlan Software A/S’s support and development services, comprising the design and implementation of controls as stated in the description. TimePlan Software A/S’s description refers to the controls established to ensure the support and development services, which TimePlan Software A/S offers to their customers (general IT controls). For a further description of services offered, please refer to section 3.

This report is prepared using the carve-out method and does not cover general IT controls that are carried out by TimePlan A/S’s sub-service providers. For customers who has an agreement for hosting, two sub-service organisations are used for hosting customer environments. Our audit did not extend to the services provided by the sub-service organisations: Itadel A/S and Mitcom A/S. The hosting services provided by Itadel A/S and Mitcom A/S include, but are not limited to:

- Physical security of data centres including environmental security and network.
- Internal user administration performed on the hosting companies’ own users, including administration of privileged access to servers and databases with access to client data.
- Logical security, including managing password policy for servers and databases.
- Managing backup of customer environments, including monitoring and restores.
- Patch management of hosted servers and databases.

We have thus not assessed whether relevant controls were suitability designed and implemented at the sub-service organisations as of October 26, 2018.

TimePlan Software A/S’s responsibilities

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

TimePlan Software A/S is not responsible for processes and controls that are performed by the individual companies, with regard to the individual TimePlan installations.

Auditor’s responsibilities

Based on our procedures, our responsibility is to express an opinion on TimePlan Software A/S’s description as well as on the design and implementation 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 plan and perform our procedures to obtain reasonable assurance that the description provides a fair presentation in all material respects and that the controls have been appropriately designed and implemented at the time of our audit.

We have complied with the requirements for independence 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 complying with the code of ethics, professional standards, and applicable requirements according to laws and other regulations.

An assurance engagement relating to the description, design, and implementation of controls at TimePlan Software A/S involves performing procedures to obtain evidence about TimePlan Software A/S's description of its system and about the design and implementation of the controls. The procedures selected depend on the auditor’s judgment, including their judgment of the risk that the description is not presented fairly and that controls have not been suitably designed and implemented. Our procedures involve testing of the design and implementation of the controls we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. Our procedures also involve 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

TimePlan Software A/S’s description is prepared with a view to meeting the common needs of a broad range of customers and their auditors and may, therefore, not include every aspect of the 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 organisation 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 organisation may become insufficient or fail.

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

Basis for qualified opinion

TimePlan Software A/S has included controls under the area Supplier Service Delivery Management, with the control objectives "To ensure protection of the organisation's assets that are accessible by suppliers" and "To maintain an agreed level of information security and service delivery in line with supplier agreements". As stated in section 4.4.9. of this report, we have noted inadequate controls to a degree that the control objectives cannot be fulfilled, due to the lack of a formal service delivery contract, including a formal service level agreement and split of responsibilities on the services provided from Mitcom A/S to TimePlan Software A/S. This also extends to control "4.4.11.4 Availability of Information Processing Facilities". Consequently, the control objective "To ensure availability of information processing facilities" cannot be fulfilled.

Qualified opinion

Our opinion is based on the matters outlined in this report. The criteria we used in forming our opinion are those described in section 2. Except for the impact of the control deficiencies described in subsection "Basis for Qualified opinion", it is our opinion that:

a) The description of the general IT controls fairly presents, in all material respects, TimePlan Software A/S's controls of relevance to the support and development services to TimePlan Software A/S's customers as designed and implemented as of 26 October 2018.

b) The controls related to the control objectives stated in the description were, in all material respects, suitably designed and implemented as of 26 October 2018.

Description of controls tested

The specific controls tested and the nature, timing, and results of those tests are evident from 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 solely intended for customers who have been using TimePlan Software A/S's services and their auditors who have an understanding sufficient 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, 3 December 2018

Deloitte

Statsautoriseret Revisionspartnerselskab

M. Bagger

Thomas Kühn
Partner, State-Authorized Public Accountant

Michael Bagger
Director, CISA

2. Assertion by TimePlan Software A/S

This report is prepared for TimePlan Software A/S's customers using TimePlan Software A/S's services as well as their auditors. Our statement includes the description of the system and control environment, including controls that TimePlan Software A/S performs for customers under their contracts with TimePlan Software A/S. Our description of the processes and the controls performed is provided in Section 3 - TimePlan Software A/S's system description.

Our description as of 26 October 2018 requires that customers and their auditors have a sufficient understanding of 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 the customers' financial statements.

TimePlan Software A/S confirms that:

1. The accompanying description in section 3 fairly presents the general controls related to TimePlan Software A/S's support and development services used by customers as of 26 October 2018. The criteria for this assertion were that the included description:
    a. presents the way in which 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 which both IT and manual systems are used for managing general IT controls;
        iii. relevant control objectives and controls designed to achieve these objectives;
        iv. controls which we, in regard to the controls' design, assumed would be implemented by TimePlan Software A/S'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 to the general IT controls.
    b. does not omit or distort information relevant to the scope of the system described, taking into account that the description is prepared with a view to meeting the common needs of a broad range of customers and their auditors and therefore cannot include any aspect of controls that 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 implemented as of 26 October 2018. 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 controls identified would, if applied as described, provide a high degree of assurance that those risks did not prevent the achievement of the stated control objectives; with the exception of the area Supplier Service Delivery Management, with the control objectives "To ensure protection of the organization's assets that is accessible by suppliers" and "To maintain an agreed level of information security and service delivery in line with supplier agreements". As stated in section 4.4.9. of this report, inadequate controls to a degree that the control objectives cannot be fulfilled have been noted. This is due to the lack of a formal service delivery contract, including a formal service level agreement and split of responsibilities, on the services provided from Mitcom A/S to TimePlan Software A/S. This also extends to control "4.4.11.4 Availability of Information Processing Facilities". Consequently, the control objective "To ensure availability of information processing facilities" cannot be fulfilled.

Aalborg, 3 December 2018
TimePlan Software A/S

Henrik Baasch
CEO

3. TimePlan Software A/S’s system description

3.1 Overview

The purpose of this description is to inform the customers of TimePlan Software A/S and their auditors about the systems in place at TimePlan Software A/S 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 also serves to inform about the controls in use to secure a safe and stable operation of the services offered by TimePlan Software A/S.

3.2 Introduction

TimePlan Software A/S is an innovative and international market leading software company that develops, markets, implements and provides support on TimePlan - the leading software for Employee Scheduling, Time & Attendance and HR Administration.

The company was founded in Aalborg in 1990, and today it has 35 dedicated employees. In addition, TimePlan Software A/S has resellers in Norway, Sweden, Finland, Germany, Holland, England and Singapore.

The first version of TimePlan was launched in 1995 in collaboration with HK, Danish Trade & Service and leading Danish retailers. Today, more than 400 companies use TimePlan in 25 countries from all types of industries in local languages, complying with the collective agreements and labour regulations.

Many of TimePlan Software A/S's customers are large, international companies with thousands of employees within the service sector, including retail, hotels, airports, amusement parks, catering companies, transportation, supplies, etc. TimePlan provides its customers with an overview and helps them save work hours and payroll costs while increasing employee satisfaction.

Thanks to the continuous and innovative development of the software and in close collaboration with the company's customers through more than 20 years, TimePlan continues to set the standard on the market for an increasing number of industries. TimePlan Software A/S listens to the wishes and needs of its customers when it comes to the development and implementation of new functionality. Over the years, the company has developed a wide range of customer-specific solutions - always focusing on data security and compliance with local rules and regulations.

Customer security is our priority at TimePlan Software A/S. All new features in TimePlan, and the entire TimePlan program, are always launched and operated in accordance with the rules and changes on the market, most recently the new EU General Data Protection Regulation (GDPR).

TimePlan Software A/S has been awarded the AAA Gold Diploma for Highest Creditworthiness, and in 2017, the company was voted No. 3 on Computerworld's list of leading IT companies in Denmark.

TimePlan Software A/S's core values are:

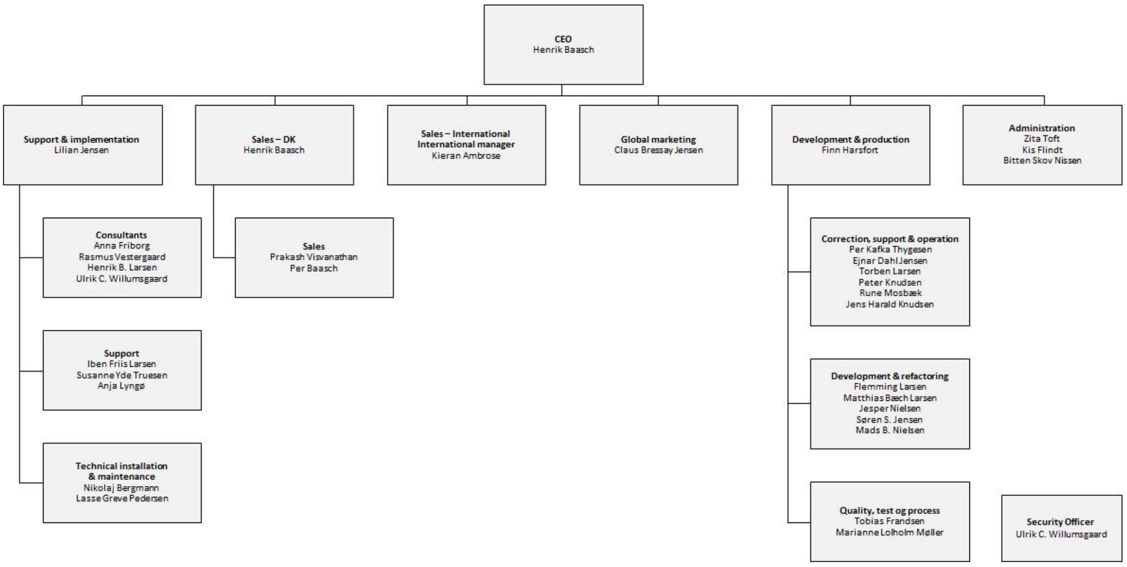
- Persistence
- Tolerance
- Honesty
- Communication
- Knowledge.

TimePlan Software A/S’s core services:

- TimePlan
- Software updates
- Software development
- System support
- Technical support
- Training in the use of TimePlan.

3.3 Organisational structure

Organisation chart of TimePlan Software A/S as of 1 October 2018:



3.4 Risk management at TimePlan Software A/S

TimePlan Software A/S uses a risk management system that consists of identification, analysis and management of risk factors in several areas and on numerous levels. Risk analysis plays a crucial role in the development and maintenance of security procedures, including the collaboration with third parties, which are reviewed at least once a year. The focus of risk management is to prevent and minimise all risks that may cause operational or security issues for TimePlan Software A/S' customers.

Input for the execution of the procedures is obtained throughout the organisation. The process is facilitated by an IT Administrator, together with the Information Security Officer who draws up drafts for management to review.

3.4.1 Procedures

Procedures are maintained on a continuous basis to comply with all existing requirements and the operational environment. Risk management is an integral part of all development procedures and is part of all service level agreements with third-party service providers. In connection with major projects, depending on the extent and severity, safety assessment and risk management are based on ISO27001 best practices. At the operational level, all projects are subject to ongoing risk management, as defined in our project management model. The responsibility for project-related risk management lies with the nominated project manager, but also involves the project participants and steering group.

3.4.2 Risk management control

TimePlan Software A/S carries out annual risk analysis complimented by the review of existing analysis when the basis for these changes are determined. In addition to the general risk management control system, there is a control framework for project monitoring under TimePlan Software A/S's Security Policy. The Security Policy covers all systems and services offered to customers and is subject to ongoing auditing.

3.4.3 Repeated processes

- Annual risk and threat assessments for the entire organisation.
- Annual review of all procedures to ensure concise documentation, optimal workflows and compliance with security policies.
- Inspection of internal procedures conducted by external auditors in relation to ISAE3402 audit.

3.5 Control framework

TimePlan Software A/S's information security policy includes all procedures and processes included in the TimePlan program and the services offered. TimePlan Software A/S is actively working to continuously improve the information security when it comes to services and software offered and do so by improving and maintaining all documented procedures. There will be ongoing internal and external reviews of procedures and general information security measures.

The overall control framework is based on ISO27001 Annex A, and is as follows:

- A.5 Information security policies
- A.7 Human resource security
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operations security
- A.13 Communications security
- A.14 System acquisition, development and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance.

3.6 Control measures

Control measures at TimePlan Software A/S are based on ISO27001 best practices and they cover several of the main areas of Annex A. ISO27001 forms the basis of the Information Security Management System (ISMS) at TimePlan Software A/S and provides the necessary discipline and responsibility for information security. The control environment serves as a management system for information security and ensures that TimePlan Software A/S maintains safe and stable operation for its customers.

3.6.1 A.5 Information Security Policy

TimePlan Software A/S's Information Security Policy is based on our ISMS and thus subject to TimePlan Software A/S's control systems, which are based on ISO27001. The Information Security Policy has been communicated to all relevant parties, and the policy is revised annually when the basis for policy changes are agreed to ensure continued stability, precision and efficiency.

The Information Security Officer (see 6.2) continuously collects and identifies the risks for which it may require an update of the policy. Once a year, proposals are submitted to the management team, and they are finally executed following a management decision. The Information Security Policy, like the other defined working procedures, is version-controlled. The management is responsible for the Information Security Policy.

All employees are presented with the Information Security Policy and amendments therein.

TimePlan Software A/S has established an internal organisation responsible for managing and implementing information security. The Management has appointed an Information Security Officer who manages tasks that fall under ISMS in collaboration with the Management.

The Management, who is the primary responsible party for IT security, ensures that there is continuous support and development of procedures and systems, which support the IT security policy, and that they are implemented daily by the Department Managers. The Department Managers ensure that procedures are followed and that any changes are announced and incorporated at regular department meetings.

3.6.2 A.7 HR and Employee Security

TimePlan Software A/S's requirements for compliance with information security and confidentiality include employee screening (including criminal record and conversations with references), Non-Disclosure Agreements (NDA) between the employee and TimePlan Software A/S, as well as approval from the Management. For projects or high-level security customers that have special security requirements, individual employees may be given official security approval by the relevant authorities.

Throughout the recruitment process, relevant applicants are screened, and it is determined whether the applicant is suitable to be employed - legally and in terms of skills and experience. Applicants who continue in the recruitment process are presented with TimePlan Software A/S's IT security approach and the privacy aspect, which constitutes the foundation for the organisation's business.

New employees are informed about the Information Security Policy and the company's core values, including a staff manual. New employees are only granted access rights according to their position, duties and responsibilities. The employee's basis of employment and reference letters are stored throughout the employment relationship as part of the employee's electronic journal.

The employees of TimePlan Software A/S are regularly informed about IT security awareness and how confidential and personal data should be handled. The Management presents all employees with the information policy. If an employee violates TimePlan Software A/S’s internal guidelines, the management can chose to use disciplinary sanctions.

When it comes to the termination of an employment relationship, the employee's rights and accesses are removed, and all company property is to be returned. They are then reminded of their obligations to their continued confidentiality after the termination of employment.

3.6.3 A.9 Access control

TimePlan Software A/S' employees are informed about their responsibilities, confidentiality rules and access authentication rules. TimePlan Software A/S and its employees will always act in accordance with EU legislation and local laws regarding access to personal information. Standards and control frameworks from ISO27001 are used as the basis for all data and system access policies. This is done to ensure a uniformed process throughout the organisation. Access management ensures that the employee has access to systems and information that is relevant for carrying out their specific tasks.

3.6.3.1 Internal access

It is TimePlan Software A/S's policy that employees should have easy and secure access to the information relevant to their functions, and that the information is structured according to company guidelines and procedures.

All access and system user rights are subject to annual audits, including, but not limited to, the following areas:

- System and server access
- Access to shared information (electronic and physical)
- Network segmentation
- VPN access.

Access to systems is limited in scope, and AD with Group Polices has been set up to control access and security. Rights allocation takes place in relation to the position and work function assessed by the individual Department Manager. Verification of rights allocation is ongoing. Rights are assigned or restricted according to needs defined and maintained by the Department Manager and executed by the IT Administrator.

The IT Administrators are the only persons who have access to make changes and implement rights. In the JIRA journal system, a case is created for the assignment or limitation in order to document a specific course of action.

If a project or task requires access or changed rights, the Department Manager may provide temporary or partial access.

On an annual basis, the Department Manager and the IT Administrator review the rights granted and ensure that the rights are correct. They must also ensure that the documentation for this is clearly stated on the employee's 'identity card', if they differ in relation to the normal restrictions.

TimePlan Software A/S has a described and incorporated password policy that defines the framework for authentication on all platforms. Passwords will expire within a system-defined timeframe and in addition to centrally controlled deletion rights, a corresponding set of rules for the quality of authentication have been set up.

3.6.3.2 External access to network (guests and consultants)

External access for guests is managed on a separate network from TimePlan Software A/S's operating environment and is limited to Internet access. External consultants do not have direct access to systems or folders without permission from the Management, and they are always obliged to sign the relevant privacy statement and undergo the same security screening procedure as in a recruitment process.

External consultants can never access customer data, systems or information, and they can never access any code libraries that reveal TimePlan's core functionality.

Access to networks and the like is closed to outsiders. Wi-Fi networks can be accessed in DMZ and are secluded for access to internal systems. Mobile devices, other than PC equipment, supply access to the separate network. There are defined system processes to ensure that mobile devices do not access the system network.

3.6.3.3 Access to customer systems (hosted)

TimePlan Software A/S views hosted customer environments, data and confidential information as the client's property, and access to these must therefore be authorised and approved by the customer. TimePlan Software A/S has access to customer assets and implements necessary security measures. This is based on the customer's instructions as the Data Controller, where TimePlan Software A/S is considered the Data Processor.

Access to a customer’s system requires that the customer defines access to the installation. Support access is thus limited and will be defined within the security policies that the customer defines and follows in the organisation's own business. TimePlan’s support access and actions are logged directly in the customer's own installation. The connection documentation is maintained according to the customer's preferences.

Customer information, including databases used by TimePlan Software A/S for development or quality control, is scrambled/anonymized, so that it is not possible to read or derive personal or company-recordable data. This is done only in agreement with the customer.

3.6.3.4 Access to customer systems (not hosted)

TimePlan Software A/S offers support for local installations in customer environments. To support these installations, TimePlan Software A/S must have remote access to the customer's server and workstation. The type and availability of these systems are maintained and controlled by the customer. Therefore, TimePlan Software A/S has no direct way to secure the network security at the customer's location. The supported user access is logged directly in the customer's installation.

Remote Access documentation and passwords are the responsibility of TimePlan Software A/S and are thus treated in accordance with TimePlan Software A/S's Control Measures Policy (especially Section

6.4). The rules are stipulated in the customer's SLA agreement. In addition, the installation is accessed through a logging environment ‘RoyalTS’, where the correct access method has been set up and defined by the customer. This logs the connection and access of each supporter, which is archived.

3.6.4 A.10 Cryptography

Cryptography is an important tool in relation to TimePlan Software A/S's Information Security Policy. Cryptography is used to secure sensitive, stored data and is used in many places in TimePlan, so customers can better secure their system (for example using biometric login and password encryption).

Encryption is used in different ways on the TimePlan platform, based on security-specific assessments, where it is considered necessary to comply with -in particular - personal data legal obligations. Encryption is used where data can be considered confidential or personally sensitive in the administration of TimePlan, protection can be applied on selected fields within the software, where relevant.

3.6.5 A.11 Physical security and environmental protection

3.6.5.1 Local physical security

Local servers and networking devices are only physically accessible to authorized persons (currently only the System Administrator and CEO). All local servers are protected by UPS (to protect against power cuts), hardware firewall, centralised antivirus software and privileged access rights. All employee computers are protected by anti-virus programs with automatic updating, AD authentication and encryption of relevant drives.

According to TimePlan Software A/S's procedure for Removable Device and Drives (phones, USB drives), external equipment cannot be connected without documented acceptance by the IT Administrator. Mobile devices are excluded from being able to connect internally, drives being scanned for malware and USB keys should, if they transport confidential material, be encrypted, for example, with BitLocker.

TimePlan Software A/S's employees are required to keep all critical data on local TimePlan Software A/S servers, which are regularly backed up in accordance with applicable procedures.

Designated employees have keys that are provided by Management that can provide access to server rooms. In addition, confidential and personal information are stored in locked cabinets. Access key delivery is registered in TimePlan through signed logging documents for issuance and return.

The company offices are secured with professional access control with a direct line to the Fire Department and Police. There is SKAL security on the building and surveillance of access and exit points. Guests are required to enrol in a 'guestbook' upon arrival and departure from the building.

The server room is equipped with smoke and temperature sensors coupled with the fire monitoring systems. Heat development in the server room is monitored and regulated by a cooling system. Once a year the IT administrator will look through all cables to ensure that proper cabling is used.

3.6.5.2 Hosted security

All third-party hosting companies that host TimePlan as part of an agreement between TimePlan Software A/S and a customer must comply with the ISO27001 standard and comply with the legal requirements for the handling of personal data, which will require documented evidence. Before contracts can be signed, the supplier's latest security review will be reviewed and a Data Processing Agreement is always drawn up with a Data Processor.

TimePlan Software A/S annually reviews the supplier service, during which time the supplier must document their information security practices, where these practices must be acceptable in relation to their own obligations towards the customers. If the compliance documentation does not comply or is insufficient, the supplier must conduct an external information security audit or update the audit report. Should the documentation be incorrect the supplier’s contract must be terminated.

TimePlan Software A/S's customers annually receive access to TimePlan Software A/S's latest auditor approved control report on the company's extranet.

3.6.5.3 Control of assets

The physical and digital assets of TimePlan Software A/S included in the provision of services are identified, registered and assigned to an owner. The information is classified in accordance with the applicable legal requirements, the value of the information and the sensitive information in relation to unauthorized access or changes. Removable media such as backup tapes and hard disks are stored in secure locations and there are procedures for safe use, transportation and disposal.

In order to avoid loss, damage, theft or compromise of assets and operating interruptions within the organization, all hardware and software is monitored through centralized software, which is reviewed as a minimum on a monthly basis. Here, versions, equipment and space are checked to ensure optimal operation. Alarms are set on essential assets to ensure optimal operation and security that allows proactive action.

The transfer of confidential information is encrypted. Recognized methods of encryption, such as BitLocker, are used. Unused hardware is effectively destroyed or, if possible, recycled for secure low-level data wipe.

3.6.6 A.12 Operational security

3.6.6.1 Tools and environment

TimePlan Software A/S's policy on Software Tools and Environment is, where possible, to run the latest versions to ensure compatibility and security. All third-party software must be approved by the Management before it can be installed. The responsibility for software and licenses lies with the Management who can delegate to the system owners. The software list is reviewed annually by the Department Manager and IT Administrator.

A thoroughly prepared positive list ensures that only required and approved software is used. The positive list is compared with installed software through the central monitoring software. Unauthorized software will be uninstalled.

A centralized management of anti-malware software has been set up that ensures latest versions, a unified policy and scan rate. GPO policies have been set to ensure optimal operation, maintenance and uniformity in security measures such as passwords, access and protection.

The Management ensures that hardware changes or acquisitions are made in accordance with the company's needs and with emphasis on optimal operation and value. The management together with the IT Administrator and possibly a third-party provider decide how changes are implemented and tested. The documentation is maintained by the IT Administrator.

TimePlan Software A/S continuously assesses the need for firmware updates on the network and communication software. Replacement and updates take place according to functionality, necessity and needs and are handled by the IT Administrator.

Systems are set for automatic updating, while possible restart is controlled by the IT Administrator to work within the service windows that are set up.

During the update of server systems, which can affect customers' operating environment, the customers receive a notification via email within a reasonable timeframe for the contact(s) that the customers have informed TimePlan Software A/S of. TimePlan Software A/S also communicates essential service releases and software news.

3.6.6.2 Development

The development environment at TimePlan Software A/S complies with the general policies as well as a set of code security and integrity procedures based on the principles of ISO27001. The focus of the development operational security policies is to protect the source code against exposure, theft and abuse.

On an operational level, the environment is ensured, as the code is stored in a version control system, moreover, regular code, environment backups as well as a complete copy are deposited offsite.

All development is documented in the record system, where employees document all tasks in the development process on a given case. Code changes are not released until they are reviewed by a secondary developer and they have undergone the nightly regression tests.

In the record system, workflows have been set up for corrections, changes and improvements. Workflows cannot be overridden in the system and require validation prior to release and operation. It is not possible for the individual developer to update or change code for release without involving other developers in the approval process.

3.6.6.3 Software test

It is TimePlan Software A/S's policy that all versions of TimePlan are tested prior to release. The test scenarios include all modules in the software and consist of several hundred regression tests performed each night as well as performance, export, statistics and payroll tests. All versions are signed by the Quality Department, the Development Department and the Management before they can be released to the customers.

3.6.6.4 Operation

The basis for operating procedures of TimePlan covers implementation, support and operations on both hosted and local customer systems, as described in the SLA between TimePlan Software A/S and the customer. All operational SLAs contain details about reliability, incident control and service windows. In hosted agreements, TimePlan Software A/S accepts all environmental obligations relating to operational reliability, with the exception of user rights and information management within the customer's installation.

Operation, test and development environments are separated, so operation is continuous and susceptible to the least possible degree.

3.6.6.5 Backup

TimePlan Software A/S and third-party hosting companies are directly responsible for correct and secure backup of all hosted systems. If the environment is hosted by third-party companies, TimePlan Software A/S is responsible for ensuring that the third party complies with TimePlan Software A/S's standards for secure hosting of software and that it is documented.

Backup and snapshots are taken continuously, ensuring continuous operation and the ability to re-establish operations quickly. It is checked and ensured that the backup is made flawlessly, and any errors are assessed and followed up. Back-up procedures are described and are an important part of the daily operations. The backup system is divided into alternate locations in relation to the operating environment.

Backup is tested continuously, as backups are used to re-establish customer data. The development environment and internal operations are part of the back-up procedures. The re-establishment plan is tested annually and serves as the basis for the contingency plan. Any necessary fixes and enhancements are versioned into the contingency plan and backup descriptions. The IT Administrator carries out maintenance and testing, and corrections are made in collaboration with the department managers.

3.6.7 A.13 Communications security

TimePlan can communicate with multiple third-party systems, such as digital signature providers. TimePlan Software A/S is responsible for allowing customers to use and access the communication opportunities provided by the platform in a safe way. Therefore, secure means of communication are always available when integrated with other systems, and all development procedures require that only secure communications protocols are being used.

Work streams have been defined in the development procedures to ensure that communication and data exchange can take place within secure protocols. The exchange is reviewed as a natural part of a code review.

3.6.8 A.14 System acquisition, development and maintenance

TimePlan Software A/S works purposefully and always with 'privacy by design' in the continuous flow of developing, strengthening, implementing and supporting legislation, security and customer wishes. Thus, TimePlan Software A/S constantly seeks to strengthen and, if necessary, improve the tools in TimePlan to provide a system that customers experience as being in sync with the latest trends within development and security that also complies with the current legal and collective requirements.

In TimePlan Software A/S, it is a focal point that the customer has the opportunity to contribute to the development of the system. This can be done in tests or through actual customer wishes that are developed and tested in collaboration with the individual customer.

Developments, fixes, improvements and changes occur according to documented workflows where components are not released before description, clarification, encoding, code review and system-flow tests have been made.

3.6.9 A.15 Supplier relationships

Before establishing a working relationship, the supplier's services and the latest security audit will be reviewed. It is assessed whether the supplier meets the same information security standards, such as TimePlan Software A/S and the organization's obligations to the customers. If this is not the case, an alternative must be found. This review is carried out by the IT Administrator and the Information Security Officer. If a cooperation agreement is made, a Data Processing Agreement will be prepared.

The delivery agreement must include the required information security requirements, including backup and supply chain structure to achieve maximum operational stability.

In the same way, the suppliers' services are reviewed annually, and documentation is obtained for compliance with the relevant information security requirements. If the supplier fails to comply with the Agreement and the documentation required, a subsequent review will be carried out and should this not produce the necessary results a replacement for the supplier must be found.

A hosting provider enters into a Data Processing Agreement with TimePlan Software A/S and is thus acquainted with the data content and the need for complimenting information security.

3.6.10 A.16 Information security incident management

TimePlan Software A/S is committed to preventing unauthorized access to TimePlan Software A/S's and customer's data and focuses on information security in both risk management and procedures.

Procedures and report forms have been created to counter any event. The incident is reported, and the immediate leader assesses together with the Information Security Officer if a Steering Group should be called to follow and act in the process.

The management of the information security breach takes place within the Steering Group with contributions from relevant parties, internally and externally. Regular information is gathered while the priority is to stop the event. TimePlan Software A/S will internally generate an incident report that will reduce the likelihood and impact of future events and, if possible, optimize the handling of such events.

The record system provides the basis for documenting a timeline in the process where relevant parties and stakeholders contribute with knowledge and execution. The priority is always to limit the damage as soon as possible.

Any information security weaknesses that are detected are reported internally and prioritized immediately.

3.6.10.1 Illegal access to secure information

In case of hacking, DDOS or similar events involving TimePlan Software A/S or a hosted customer, TimePlan Software A/S will take immediate action and identify, isolate and remove any vulnerabilities. TimePlan Software A/S will report all illegal access events to the relevant authorities and where appropriate customers, who will assist in any relevant investigations.

If a security breach occurs, the risk is assessed and the measures necessary for the situation are initiated to stop the attack, clarify the situation and communicate with the relevant stakeholders. Report forms have been prepared in accordance with the requirements of the General Data Protection Regulation (GDPR).

3.6.11 A.17 Information security aspects of business continuity management

TimePlan Software A/S is committed to addressing all potential threats with a policy for prevention and resolution if a threat is considered serious and/or likely. If a crisis occurs, TimePlan Software A/S will launch the corresponding crisis management procedure to resolve and fix the problem immediately. Procedures and contingency plans are reviewed annually and whenever the basis of current plans is changed.

At TimePlan Software A/S, there is a contingency plan in place in case of a breakdown. The contingency plan forms the basis for reinstatements or the like and sets out the framework for contact and action. Elements in the plan are tested continuously - either as a desktop test or in connection with data restitutions.

The contingency plan has been approved by the Management and it ensures the process of restoration and remediation. In operating environments, continuous operation and uptime are guaranteed by redundancy, load balancing, mirrored systems and hardware.

3.6.11.1 Internal crisis

In case of an internal crisis (such as server loss), TimePlan Software A/S will initiate emergency procedures to minimize customer impacts, including load balancing of systems until normal operations are restored.

Hosting providers have defined procedures for handling system failures, which are initiated if necessary. The IT Administrator follows the process and reports internally to the Management.

3.6.11.2 Customer crisis

In case of a customer crisis, such as data loss, TimePlan Software A/S will assist the customer with re-establishment. Individual SLAs can define a framework for crisis management, and if so, this will be the basis for the crisis management. TimePlan Software A/S has standardized procedures with detailed crisis management derived from risk management assessments that will be followed, unless otherwise specified in the SLA.

TimePlan Software A/S will assist the customer in restoring its operating environment as soon as possible. System and data restoration are part of the ongoing emergency testing.

3.6.11.3 Supplier crisis

In the event of a major incident regarding external hosting by one of TimePlan Software A/S partners, TimePlan Software A/S will work closely with the hosting company concerned to restore a working environment for all affected customers as quickly as possible. Afterwards, TimePlan Software A/S will make the necessary improvements to the hosting environment to prevent future outages.

TimePlan Software A/S uses two hosting providers, which ensures thorough restoration of backups and systems. The operational environment of a given provider can be moved or re-established alternatively. The re-installation is tested at the supplier on an annual basis.

3.6.12 A.18 Compliance

TimePlan Software A/S conducts an annual review of internal procedures where management assesses whether information security is implemented and they review the operativeness of the procedures. There is also a technical compliance review in place to ensure that the TimePlan system is in compliance with technical and security requirements. Furthermore, an external review of the procedures implemented by TimePlan Software A/S is performed in relation to the ISAE 3402 audit to ensure compliance.

3.7 Additional information on the control environment

The following matters should be considered by the customers' auditors.

User access management

Administration of users (creation, deletion, review and control of access rights) within the TimePlan application is the responsibility of the clients, and the client auditors should therefore assess these controls locally, when considering the overall control environment.

Testing of changes

TimePlan Software A/S supplies general releases for the TimePlan software. Customers and their auditors should themselves assess whether it is needed to test integrations or special setup on the customer side for new releases, to ensure that the specific release works in the specific customer setup, based on an assessment of risks of misstatements in the financial reporting.

Sub-service organisation auditor statements

As a part of the control environment for hosted clients is outsourced to sub-service organisation, the customers with a hosted TimePlan solution should obtain and review the auditor statements from the sub-service organisations, to assess whether controls are adequate in terms of risk of material misstatements.

4 Information provided by Deloitte

4.1 Introduction

This outline has been prepared in order to inform customers of controls performed by TimePlan Software A/S that may affect the treatment of accounting transactions and to state the design and implementation 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 in the planning of 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 TimePlan Software A/S.

Our testing of TimePlan Software A/S's controls is limited to the control objectives and related controls referred to in the test table below and it is not extended to include all of the controls described in the management's description of the system. In addition, controls performed at the premises of TimePlan Software A/S'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 written using the carve out method and does not cover any controls performed by the subservice providers Itadel A/S and Mitcom A/S, as this is the responsibility of the hosting provider per the hosting agreements. These controls include, but are not limited to, controls around physical and logical security, network controls, backup, user administration and patch management on the hosted environments.

Finally, the customers may have established compensating controls that help minimize the control weaknesses referred to in this report to a level acceptable for audit purposes. Such an assessment can only be made by the customers and their 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 TimePlan Software A/S's documents and recordings. The control environment was assessed in order to determine the nature, timing and scope of controls and the design and implementation of those controls.

4.3 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 might have identified.

4.4.1 A.5 Information security policies

Control Activity	Client 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 *Security policy*	TimePlan Software A/S has prepared an IT security policy, covering relevant IT security-related guidelines. The policy has been approved by the management and is published via the TimePlan app, where employees are required to read and accept the policy.	Deloitte has observed that the security policy exists and has verified that it has been approved by management. Deloitte has inspected for one sample that the IT security policy has been read and accepted by an employee. Furthermore, Deloitte has observed that the IT security policy is published on the intranet.	No deviations noted.
4.4.1.2 *Review of the policies for information security*	TimePlan Software A/S performs a periodic review of the IT security policy and the corresponding risk assessment when significant changes occur. Changes will be approved by management.	Based on interviews and documentation, Deloitte has assessed that there is a procedure in place for a yearly review of the IT security policy.	No deviations noted.

4.4.2 A.7 Human resource security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered			
4.4.2.1 *Screening*	All applicants are screened according to defined screening criteria and relevant laws. For all hires, criminal records are obtained and archived on the employee master record in TimePlan according to the procedure.	Deloitte has observed that a screening procedure for screening is in place, describing how the background check is performed. Deloitte has inspected for one sample that a criminal record was collected and uploaded to the employee's master record in TimePlan.	No deviations noted.
4.4.2.2 *Terms and conditions of employment*	For all new hires a contract for employment is made between TimePlan Software A/S and the employee, stating the terms and conditions of the employment. The contract for employment contains a confidentiality agreement.	Deloitte has observed that a procedure for setting terms and conditions is in place, specifying that contracts shall be in place for all new employees. Based on a sample of one employee Deloitte has inspected that a contract for employment is made covering terms and conditions of employment, and that a confidentiality agreement has been signed.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that employees and contractors are aware of and fulfil their information and security responsibilities			
4.4.2.3 *Management responsibilities*	Department managers have the responsibility to ensure compliance with the IT security policy as well as the policies relevant for their department. Furthermore, management has appointed an IT security responsible.	Deloitte has observed that a policy stating management responsibility for compliance with procedures is in place. Deloitte has inspected that roles are defined on the organisational chart and that an IT security responsible is appointed.	No deviations noted.
4.4.2.4 *Information security awareness, education and training*	TimePlan Software A/S's management requires all employees to have read the information security policy and comply with the policy in their daily work as stated in the employee handbook. On a periodic basis, employees are made aware of IT security risks via emails.	Deloitte has observed that a procedure for information security awareness and training is in place. Deloitte has inquired whether IT security awareness education is performed on a periodic basis and inspected a sample of the awareness emails.	No deviations noted.
4.4.2.5 *Disciplinary process*	If a TimePlan Software A/S employee violates internal guidelines, the management will decide if disciplinary sanctions should be applied and the relevant sanctions will be determined based on the violation.	Deloitte has observed that a procedure for disciplinary sanctions is in place and that management responsibility is defined within this procedure.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
4.4.2.6 *Termination or change of employment responsibilities*	When a user resigns or is terminated, the user rights are removed and all equipment must be returned to TimePlan Software A/S. Employees will sign a declaration stating that the employee does no longer have access to client information.	Deloitte has observed that a procedure for terminations and change of employment responsibilities is in place and that it specifies that all access shall be removed. Deloitte has inspected for one sample that access is removed and that a declaration is signed.	No deviations noted.

4.4.3 A.9 Access control

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To limit access to information and information processing facilities			
4.4.3.1 *Access to networks and network services*	Access to network resources is approved by a department manager, and network access is allocated based on a work-related need.	Deloitte has observed that a procedure for access to networks is in place, specifying that only users with a work-related need can be assigned access. Deloitte has inspected the access list for core network equipment and has assessed that access to the joint user is appropriately restricted to a few internal employees.	No deviations noted.
Control Activity	**Client Control Activity**	**Audit Procedures Performed**	**Test Results**
Control objective: To ensure authorized user access and to prevent unauthorized access to systems and services			
4.4.3.2 *User registration and de-registration*	User administration procedures have been prepared, and a department manager must initiate all internal user registrations or de-registrations.	Deloitte has observed that a procedure for user registration and de-registration is in place. The procedure specifies that this process is initiated by management. Based on a sample, Deloitte has assessed that the user registration and de-registration is initiated by a department manager.	No deviations noted.
4.4.3.3 *User access provisioning*	A department manager initiates user access provisioning by creating a case in Jira, and access is provided by IT administrator. All employees of TimePlan Software A/S are assigned individual and personal user profiles and have their access rights allocated based on position and department.	Deloitte has observed that a procedure for user provisioning is in place and that it covers that access is provisioned based on predefined profiles approved by a department manager. Based on a sample we noted that the user creation is initiated by a department manager, and access is provided by the IT administrator based on defined profiles.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
4.4.3.4 *Management of privileged Access rights*	Only a few selected users have administrative rights to the TimePlan Software A/S platform. Administrator access rights are approved by the management according to the user administration procedure.	Deloitte has observed that a procedure for management of privileged access rights is in place and we have reviewed the list of employees with privileged access rights. Deloitte reviewed all users with administrative rights on the TimePlan Software A/S domain and TimePlan Software A/S's managed admin users on hosted domains and verified them with management.	We noted that one user has access to all internal environments and the corresponding infrastructure internally at TimePlan Software A/S. Further, we noted that developers use a shared 'sa' account on one of the hosted domains.
4.4.3.5 *Management of secret authentication information for users*	TimePlan Software A/S has created a password policy covering the internal domain, where rules regarding passwords are described. Security parameters regarding passwords on the internal network have been set up using the standard Windows password functionality.	Deloitte has performed a review of the implemented password policy on the internal TimePlan Software A/S domain and has assessed whether it complies with the baselines and security standards defined.	No deviations noted.
4.4.3.6 *Review of user access rights*	Users and their access rights for internal systems and client data are reviewed and approved by the management on a regular basis. The review is performed and documented according to the procedure.	Deloitte has observed that a procedure for periodic review of access rights is in place and that access is to be approved by the department manager. Deloitte has inspected documentation for the performance of one user access rights review and verified the results thereof.	No deviations noted.
4.4.3.7 *Removal or adjustment of access rights*	If an employee is terminated the user profile is deleted when he/she leaves the company. Management initiates the removal of rights via Jira and, based on this, system access is revoked by the IT administrator.	Deloitte has observed that a procedure for removal of access rights is in place. Deloitte tested one sample of a terminated user and we has verified that the corresponding user profile and access had been revoked.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To make users accountable for safeguarding their authentication			
4.4.3.8 *Use of secret authentication information*	TimePlan Software A/S has implemented guidelines for the use of passwords and has defined that passwords are strictly personal and have to follow the general password policy.	Deloitte has observed that a procedure for use of passwords is in place and that the procedure covers the employees' responsibility towards password management.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent unauthorized access to the system			
4.4.3.9 *Secure logon procedures*	Security parameters regarding passwords on the internal network have been set up using the standard Windows password setting. Access to other systems is validated through Windows AD credentials. External access is validated through VPN.	Deloitte has observed that a procedure for secure login is in place. Deloitte has observed that access on the TimePlan Software A/S internal domain is governed by passwords and we have observed, from one sample, that access from external network is validated via VPN.	No deviations noted.
4.4.3.10 *Password management system*	TimePlan Software A/S has established a procedure defining rules on how employees secure passwords. Sharing a personal password is considered breaking the information security and will be handled through the disciplinary process. Standard passwords are stored in a restricted safe.	Deloitte has observed that a procedure for password management is in place. Deloitte has inquired with key personnel and has verified the storage procedures for standard passwords.	No deviations noted.
4.4.3.11 *Use of privileged utility programs*	Allocation of rights for privileged accounts and accounts directed towards client environments is restricted to employees with a work-related need only. A TimePlan Software A/S employee must obtain a formal approval from the customer before accessing the customer environment. All access from the TimePlan Software A/S domain to customer environments must be logged as a case in Jira.	Deloitte has observed that a procedure for using privileged access rights is in place and that the procedure covers access towards customer environments. Based on one sample, Deloitte has inspected that a customer approval was in place for access to a customer environment.	No deviations noted.

4.4.4 A:10 Cryptography

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information			
4.4.4.1 *Policy on the use of cryptographic controls*	A formal policy on the use of cryptography has been issued. The policy defines the types of algorithms the TimePlan software uses for cryptography and the encryption programs that the employees are allowed to use.	Deloitte has observed that a procedure for encryption is in place and verified, for samples of extracted data from the database, that the data in TimePlan was encrypted.	No deviations noted.
4.4.4.2 *Key management*	A formal policy on storage of encryption keys has been issued to ensure that keys are appropriately stored.	Deloitte has observed that a procedure for key management is in place.	No deviations noted.

4.4.5 A.11 Physical and environmental security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent unauthorized physical access and damage to and interference in the organisation's information and information processing facilities.			
4.4.5.1 *Equipment siting and protection*	The development environment and test servers are located in the server room at Vandmanden 10. Access to the server room is restricted and only authorized personnel has access to the key.	Based on inspection of the server room and inquiry with key personnel, Deloitte has assessed that access to the server room is restricted as described.	No deviations noted.
4.4.5.2 *Supporting utilities/* *Environmental mechanisms*	The following environmental mechanisms are installed at TimePlan Software A/S's location at Vandmanden 10: • Alternative power (UPS) • General fire alarms • Cooling. All environmental security mechanisms are subject to regular maintenance, service and testing.	Deloitte has observed that a formal policy is in place for maintaining utilities supporting requirements for external systems as well as internal systems. Deloitte has inspected the server room at Vandmanden 10 and noted that UPS is installed and fire alarms are set for the entire building. Further, Deloitte has assessed the documentation regarding internal testing of UPS.	No deviations noted.
4.4.5.3 *Cabling security*	All power and internet cables are examined yearly, and in case a cable change is required, a case is created in Jira.	Deloitte has observed that a procedure for cabling security is in place and inspected one sample of the yearly check of cables had been performed according to the procedure.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
4.4.5.4 *Equipment maintenance*	All equipment is identified and registered in the monitoring system, allowing TimePlan Software A/S to monitor all servers, clients and installed software. The IT administrator performs periodic follow-ups to ensure that software is up-to-date.	Deloitte has observed that a procedure is in place for maintenance of equipment covering both software and hardware. Deloitte tested a sample to determine whether the internal domain and development server is appropriately patched.	No deviations noted.
4.4.5.5 *Removal of assets*	Assets owned by TimePlan Software A/S must only be removed from the head office following the approval of the management. All assets containing sensitive data must use encryption.	Deloitte has observed that a policy on removal of assets is in place, and that the policy covers management approval to remove assets.	No deviations noted.
4.4.5.6 *Security of equipment and Assets off-premises*	Home offices for TimePlan Software A/S employees are set up with approval from the CEO.	Deloitte has observed that a policy for security of equipment and assets off-premise is in place, which covers assets at the external hosting companies and assets located at employees' home offices. Based on inquiry with key personnel, we noted that the number employees with home offices is limited to one employee. We noted that this is approved by the CEO.	No deviations noted.
4.4.5.7 *Secure disposal or reuse of equipment*	All disposal of equipment shall happen in a secure way where all hard drives are wiped and destroyed. Equipment is subject to reuse and in this case, certain measures need to be taken to ensure that information cannot be retracted.	Deloitte has observed that a procedure for secure disposal and reuse of equipment is in place, and that the procedure covers rules for both disposal and reuse.	No deviations noted.
4.4.5.8 *Unattended user equipment*	Equipment and devices containing customer data or personally identifiable information is subject to a screensaver policy.	Deloitte has observed that a procedure for unattended user equipment is in place and that a GPO with lock screen is set up for computers in the internal domain. Mobile devices are password protected.	No deviations noted.
4.4.5.9 *Clear desk and screen policy*	A formal clear desk policy is implemented covering the TimePlan Software A/S main office. All employees have to clear their desks at the end of the workday.	Deloitte has inspected selected departments at TimePlan Software A/S's location and noted that unmanned desks were cleared.	No deviations noted.

4.4.6 A.12 Operations security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure correct and secure operations of information processing facilities			
4.4.6.1 *Written guidelines and procedures*	With foundation in ISO 27001, TimePlan Software A/S has defined written guidelines and procedures and these procedures are available to all employees on the intranet.	Deloitte has reviewed that procedures are stored on and are available to TimePlan Software A/S employees on the intranet.	No deviations noted.
4.4.6.2 *Change Management*	TimePlan Software A/S has defined formal change management procedures to control development, building and deployment processes.	Deloitte has observed that the change management procedures exist and that they are available on the intranet.	No deviations noted.
4.4.6.3 *Capacity Management*	TimePlan Software A/S has set up capacity management as well as monitoring on internal managed servers and clients. The IT administrator is responsible for following up on any alarms when exceeding set limits.	Deloitte has observed that a procedure for capacity management is in place. Deloitte inspected an extract from the capacity management system and verified that no alarms were sent for the selected sample.	No deviations noted.
4.4.6.4 *Separation of development, testing and operational environment*	TimePlan Software A/S has separated development, test and production environments on different servers. No customer environments are physically placed on TimePlan's servers on Vandmanden 10.	We have inspected documentation on the separation of development, testing and operating environments.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that information and information processing facilities are protected against malware			
4.4.6.5 *Controls against malware*	TimePlan Software A/S has installed antivirus software on all servers and clients managed by TimePlan Software A/S on the internal domain. The definitions are set to automatic updates.	Deloitte has observed that a procedure for protection against malware is in place, and that it requires antivirus software to be installed on all clients and servers internally. Deloitte has inspected for one client and one server that antivirus protection is installed, and that definitions are updated.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To protect against loss of data			
4.4.6.6 *Information backup*	Backup of the internal development servers is performed daily and backup is stored off-site. Backups are checked for errors daily, and if there are any errors, these are handled by the IT administrator in collaboration with the hosting partner.	Deloitte has observed that a procedure for backup is in place. Deloitte has obtained documentation regarding the backup strategy and verified the backup configuration. Deloitte has for one sample verified that the backup job ran successfully.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To record events and generate evidence.			
4.4.6.7 *Event logging*	Relevant user activities, exceptions and security events are logged and sent to a log-monitoring tool. Access to the externally hosted customer environments is logged and stored via Remote Desktop. In case of security violations, unauthorized attempts to access information resources, reports can be generated from the logs. Log dashboards are reviewed on a periodic basis and any violations are recorded in Jira.	Deloitte has assessed the log mechanisms and procedures regarding security logging in general. Deloitte has inspected the log dashboard used for periodic review.	No deviation noted.
4.4.6.8 *Protection of log information*	All logs are sent to the log management tool via a Windows event log in real time, where they are stored in the underlying database in a read-only state.	Deloitte has inquired with key personnel whether procedures are in place for safeguarding logs. Based on the interview and the log management tool set up, we assessed that the log setup is appropriate.	No deviation noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
4.4.6.9 *Administrator and operator log*	Administrator access is logged and sent directly to a log-monitoring tool. Every week logs are reviewed based on a predefined dashboard by a non-administrator employee. Any violations are handled via Jira.	Deloitte has assessed the log mechanisms and procedures regarding administrator logging in general. Deloitte assessed the procedure for reviewing the administrator logs.	We noted that the dashboard setup used for monitoring the administrator access only includes actions performed by a few predefined admin accounts, and thus does not include all potential critical actions performed. Further, we noted that the dashboards could be modified by a user who has admin access.
4.4.6.10 *Clock synchronization*	TimePlan Software A/S has set all servers in the internal TimePlan Software A/S domain to have clock synchronization.	Deloitte has observed that a procedure for clock synchronization is in place. Deloitte has obtained one sample to verify that there is an appropriate set-up of clock synchronization.	No deviation noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent exploitation of technical vulnerabilities			
4.4.6.11 *Management of technical vulnerabilities*	All equipment is continuously monitored via a monitoring tool to ensure that the newest software versions available are used. The IT administrator is responsible for this.	Deloitte has observed that a procedure for management of technical vulnerabilities is in place. For one server Deloitte has inspected that the server was appropriately patched.	No deviation noted.
4.4.6.12 *Restrictions on software installation*	TimePlan Software A/S has created a positive list of management-approved software allowed to be installed on clients. To ensure compliance with the positive list there is a periodic check to validate that no users have installed non-approved software.	Deloitte has observed that a procedure for restrictions on software installation is in place. Deloitte has obtained a sample review where installed software on one employee PC is compared to the positive list with no deviations.	No deviation noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To minimize the impact of audit activities on operational systems			
4.4.6.13 *Information systems audit controls*	TimePlan Software A/S has defined a formal policy-covering audit of information systems, including appointed responsible roles in relation to securing audit documentation.	Deloitte has observed that a policy for audit of information systems is in place.	No deviation noted.

4.4.7 A.13 Communications security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure protection of information in networks and its supporting information processing facilities.			
4.4.7.1 *Network controls*	Internal networks used in TimePlan Software A/S are closed and secured against unauthorized access. All access to network equipment is password protected and admin access is restricted to only a few persons. All network access in TimePlan Software A/S is logged.	Deloitte has observed that a procedure for network controls is in place and that the procedure includes rules for access to network. Deloitte has inspected the high-level network security and noted that a password is required to gain access. Further, we noted from inspection that traffic is logged, and that privileged access is limited to only a few authorized employees.	No deviations noted.
4.4.7.2 *Security of network services*	Switch and firewall at TimePlan Software A/S is manually patched by the IT administrator.	Deloitte has observed that a procedure for security of network services is in place. Deloitte has reviewed the patch management standards and tested a sample of core network equipment to establish that patches had been implemented.	No deviations noted.
4.4.7.3 *Segregation in networks*	TimePlan Software A/S's internal networks are segregated. No external or guest users have access to the internal network.	Deloitte has reviewed network documentation and noted that the internal network is segregated.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To maintain the security of information transferred within an organisation and with any external entity.			
4.4.7.4 *Information transfer policies and procedures*	If a data transfer is not covered by a data processing agreement, transfer of information to external locations or to external parties must always be approved by management.	Deloitte has observed that a procedure for transfer of information is in place and that the procedure covers rules for data transfer.	No deviations noted.
4.4.7.5 *Agreements on information transfer*	All transfers of information are governed by data processing agreements. TimePlan Software A/S has an overview of all data processing agreements with clients with an overview of all types of processed personally identifiable information.	Deloitte has inspected a sample to determine if a data processing agreement has been established between TimePlan Software A/S and a customer. Additionally, Deloitte has inspected TimePlan Software A/S's overview of all data processing agreements.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
		Finally, Deloitte inspected, that data processing agreements have been established between TimePlan Software A/S the service providers Itadel A/S and Mitcom A/S.	
4.4.7.6 *Electronic messaging*	All transfers of personally identifiable data from TimePlan Software A/S sent via electronic communication must be encrypted.	Deloitte has observed that a procedure on electronic messaging is in place.	No deviations noted.
4.4.7.7 *Confidentiality or non-disclosure agreements*	All employees in TimePlan Software A/S are subject to confidentiality. All contracts between TimePlan Software A/S and the employees include a section about confidentiality, which is further emphasized in the employee handbook. TimePlan Software A/S has made data processing agreements with the hosting companies for the customer environments.	Deloitte has observed that a procedure on confidentiality agreements is in place. Deloitte has inspected an employee contract and noted that a section about confidentiality is included. Additionally, Deloitte has verified that the employee handbook has a section regarding confidentiality. Deloitte has inspected that a data processing agreement has been established between Itadel A/S and Mitcom A/S, and that these data processing agreements cover confidentiality.	No deviations noted.

4.4.8 A.14 Systems acquisition, development and maintenance

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes requirements for information systems which provide services over public networks			
4.4.8.1 *Information security* *requirements analysis and specification*	TimePlan Software A/S has defined information security requirements as a part of the change management procedures. When a change is processed in the Jira flow, security risks are assessed, and all information security requirements are specified.	Deloitte has observed that a change management procedure is in place. Deloitte tested a change to establish that security requirements were specified and documented in the Jira flow.	The formal registration of the security risk assessment in Jira is still being implemented, thus, security assessments were at the time of the audit handled informally.
4.4.8.2 *Securing applications on public networks*	The management in TimePlan Software A/S has implemented guidelines on security when working in public networks. The guidelines define how the employee must act when they are on an open network.	Deloitte has observed that a procedure on security on public networks is in place, covering employee's use of public networks.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that information security is designed and implemented within the development lifecycle of information systems			
4.4.8.3 *Secure development policy*	TimePlan Software A/S has defined change management procedures regarding secure development, build and deployment processes.	Deloitte has observed that procedures for change management are in place and that they cover considerations on secure development.	No deviations noted.
4.4.8.4 *System change control procedures*	TimePlan Software A/S has defined a system change control procedure, which is supported by workflows in the change management system, ensuring that each step is documented.	Deloitte has observed that a system change control procedure is in place and has verified for one sample that the change management flow was adequately followed and documented.	No deviations noted.
4.4.8.5 *Technical review of applications after operating platform changes*	TimePlan Software A/S performs a code- and design review on all changes before release of a build. A release document is signed by management before the version is released to customers.	Deloitte has verified that the procedure for review of systems after changes is in place. Deloitte has verified for one change that a code- and design review was performed and that a release document was made and signed for the selected release.	No deviations noted.
4.4.8.6 *Restrictions on changes to software packages*	TimePlan Software A/S has implemented a change management process ensuring restriction of changes to software. This means that changes must not be initiated without formal approval by the CTO and without the flow being documented. No employees in TimePlan Software A/S have access to circumvent the change flow.	Deloitte has tested for one change that the process was followed and documented as described. Deloitte has reviewed access lists for all TimePlan Software A/S environments.	We noted that one TimePlan Software A/S IT administrator has access across all environments.
4.4.8.7 *Secure system engineering principles*	TimePlan Software A/S has implemented guidelines for secure development. The responsibility for enforcing the guidelines lies with the department manager in the development department.	Deloitte has verified that there are guidelines for secure development, and that it is defined that it is the responsibility of the development manager	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
4.4.8.8 *Secure development environment*	TimePlan Software A/S has separate development, test and production environments. These environments are physically placed on different servers.	Deloitte has observed that there are guidelines for secure development environments in place. Deloitte has obtained documentation regarding separation of development, testing and operational environments and has assessed that the environments are physically separated.	No deviations noted.
4.4.8.9 *Outsourced development*	TimePlan Software A/S has defined a procedure for using external consultants for development. External consultants will go through a screening process similar to internal employees before agreeing on the contract. External consultants will follow the same change management procedure as an internal employee.	Deloitte has observed that there is a procedure for outsourced development in place.	No deviations noted.
4.4.8.10 *System security testing*	Test of security functionality is carried out as a part of the change management flow. Testing will be performed by another developer and integration tests are performed nightly on the build server.	Deloitte has observed that a procedure for system security testing is in place. The procedure also includes security considerations in the review phases. Deloitte has verified for one change that design review, code review and integration testing was performed.	No deviations noted.
4.4.8.11 *System acceptance testing*	TimePlan Software A/S has defined guidelines for testing the developed solutions. All functionality is manually tested and approved before the functionality is subject to the automated nightly integration tests. No functionality with errors will be approved for final release.	Deloitte has observed that a procedure for system acceptance testing is in place. Deloitte has verified for one change that a release document has been prepared and signed for the selected release and that no errors were recorded on the release document.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure the protection of test data			
4.4.8.12 *Protection of test data*	Test data is the property of the customer, and can only be used by TimePlan Software A/S with approval from the customer. Test data is anonymized/scrambled on the test database.	Deloitte has observed that a procedure for protection of test data is in place. Deloitte has for a sample of test data inspected that test data was scrambled on the test database.	No deviations noted.

4.4.9 A.15 Supplier service delivery management

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure protection of the organisation's assets that is accessible by suppliers			
4.4.9.1 *Information security policy for supplier relationships*	TimePlan Software A/S periodically assess if the supplier is able to comply with information security guidelines, consistent with the ones set by TimePlan Software A/S.	Deloitte has observed that a procedure for information security requirements for suppliers is in place. Deloitte has inspected that a data processing agreement has been signed between TimePlan Software A/S and the suppliers Itadel A/S and Mitcom A/S.	We noted that no formally signed hosting agreement with Mitcom A/S has been prepared.
4.4.9.2 *Addressing security within supplier agreements*	TimePlan Software A/S has made data processing agreements with all suppliers who have access to relevant data. In each data processing agreement with the supplier, it is defined that the sub-data processor agrees to support the information security requirement set by TimePlan Software A/S.	Deloitte has observed that a procedure for addressing security with suppliers is in place, covering information security requirements. Deloitte has inspected that a data processing agreement has been signed between TimePlan Software A/S and the suppliers Itadel A/S and Mitcom A/S.	We noted that no formally signed hosting agreement with Mitcom A/S has been prepared.
4.4.9.3 Information and communication technology supply chain	On a continuous basis, TimePlan Software A/S follows up on information security at the hosting partners. TimePlan Software A/S performs a periodic follow-up on the requirement that the hosting partner is able to document the IT security level.	Deloitte has observed that a procedure for follow-up on service providers is in place.	We noted that no formally signed hosting agreement with Mitcom A/S has been prepared.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements			
4.4.9.4 *Monitoring and review of supplier services*	TimePlan Software A/S is performing ongoing monitoring of the services delivered by the hosting companies specified in the agreement, including backup and monitoring of servers. On a yearly basis, the suppliers are reviewed to ensure that the promised services were delivered and that the information security requirements set are complied with.	Deloitte has observed that a procedure for monitoring and review of supplier services is in place, and that this includes ongoing monitoring of delivered services, such as backup. Deloitte has inspected the formal agreements with the hosting suppliers. Deloitte has inspected a quarterly report from a supplier, on the delivered services.	We noted that no formally signed hosting agreement with Mitcom A/S has been prepared, and thus, the basis for monitoring and review of the agreed upon services cannot be performed.
4.4.9.5 *Managing changes to supplier services*	Changes to supplier services will result in a changed agreement or an addition to the existing contract. TimePlan Software A/S must not enter into supplier agreements before having thoroughly reviewed that all underlying IT security on the supplier side is acceptable.	Deloitte has observed that a procedure for managing changes to supplier contracts is in place. Deloitte has inspected formal agreements with the hosting providers.	We noted that no formally signed hosting agreement with Mitcom A/S has been prepared.

4.4.10 A:16 Management of information security incidents and improvements

Control Activity	Client 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			
4.4.10.1 *Responsibilities and procedures*	TimePlan Software A/S has prepared a procedure for information security events, where responsibility is defined.	Deloitte has reviewed the procedure for information security events and obtained the organisational chart, where the corresponding responsibilities are stated.	No deviations noted.
4.4.10.2 *Reporting information security events*	As a part of the information security incident process, TimePlan Software A/S management is responsible for reporting information security events, filling out a defined report template as soon as the event is discovered and handling the incident in a timely manner.	Deloitte observed that a procedure for reporting information security events is in place. Deloitte has selected one sample incident and has verified that the procedure was followed.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
4.4.10.3 *Reporting information security weaknesses*	Information security weaknesses will be reported to management and the IT security responsible via Jira, and a case will be documented through there.	Deloitte observed that a procedure for reporting information security weaknesses is in place, and that it covers appropriate reporting.	No deviations noted.
4.4.10.4 *Assessment of and decision on information security events*	The information security officer along with the management are responsible for the assessment of and decisions made in relation to information security incidents.	Deloitte has reviewed the procedure for the assessment of and decision on information security events. Deloitte has inspected one incident and has verified that the procedure was followed and that the appointed responsible persons were involved.	No deviations noted.
4.4.10.5 *Response to information security incidents*	As part of the information security incidents process, employees must be aware of IT security incidents and respond as timely as possible to management. An incident report is completed as soon as the event is discovered.	Deloitte has observed that a procedure for responding to information security incidents is in place, and that it covers timely and documented response to incidents.	No deviations noted.
4.4.10.6 *Learning from information security incidents*	As part of the information security incident process, TimePlan Software A/S management will share lessons learned with relevant employees, when the specific incident is closed.	Deloitte has reviewed the procedure for learning from security incidents and has verified from one incident that lessons learned are documented and shared according to the procedure.	No deviations noted.
4.4.10.7 *Collection of evidence*	As part of the information security incident process, TimePlan Software A/S will collect evidence and document incidents in Jira.	Deloitte has reviewed the procedure for collection of evidence and has verified from one incident that this was documented.	No deviations noted.

4.4.11 A.17 Information security aspects of business continuity management

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: Information security continuity shall be embedded in the organisation's business continuity management systems.			
4.4.11.1 *Planning information security*	TimePlan Software A/S has prepared a disaster recovery plan, which has been approved by the CEO. The plan supports the restoration and recovery of the internal infrastructure as well as a supplementing action plan regarding the hosted customer environments.	Deloitte has inspected the disaster recovery plan and assessed its contents in terms of TimePlan Software A/S's internal organisation and setup.	No deviations noted.
4.4.11.2 *Implementing information security testing*	TimePlan Software A/S has defined preventive and recovery measures in order to ensure business and system continuity, and has created disaster recovery scenarios to be tested.	Deloitte has observed the documentation describing the disaster recovery scenarios, which covers internal crisis, customer crisis and crises at hosting suppliers.	No deviations noted.
4.4.11.3 *Verify, review and evaluate information security continuity*	TimePlan Software A/S performs periodic testing of relevant disaster recovery scenarios as manual simulations of events.	Deloitte has observed that the disaster recovery plan contains relevant scenarios.	We have noted that some elements of disaster recovery testing have been considered. However, we noted that no full disaster recovery scenario has yet been tested.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure availability of information processing facilities			
4.4.11.4 *Availability of information processing facilities*	TimePlan Software A/S uses two different hosting companies to ensure that all customer environments can be moved to a secondary location in case of a disaster at one of the service providers.	Deloitte has reviewed the agreements with the hosting suppliers.	We noted that no formally signed hosting agreement with Mitcom has been prepared.

4.4.12 A.18 Compliance

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure availability of information processing facilities			
4.4.12.1 *Independent review of information security*	TimePlan Software A/S will engage an external auditor to perform a yearly independent review of information security, which includes a complete review of all processes.	Deloitte has observed that a procedure for independent review of information security is in place, and that it covers guidelines for audit of procedures.	No deviations noted.
4.4.12.2 *Compliance with security policies and standards*	TimePlan Software A/S performs a yearly internal review of compliance with the security policies and standards, where each appointed responsible revisit the procedures.	Deloitte has observed that a procedure for compliance with security policies and standards is in place, and that responsibility and scope for review of procedures are defined.	No deviations noted.
4.4.12.3 *Technical compliance review*	TimePlan Software A/S performs a yearly technical compliance review, where overall compliance with the information security policy is assessed for all information systems in TimePlan Software A/S.	Deloitte has observed that a procedure for technical compliance review is in place, and that the procedure covers a yearly IT security review of the entire internal platform.	No deviations noted.