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 2

Independent auditor’s report on general IT controls regarding support and development services throughout the period from 01 January 2019 to 31 December 2019

Contents

1. Independent auditor’s report

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

To: The Management of TimePlan Software A/S, TimePlan Software A/S’ customers and their auditors

Scope

We have been engaged to report on TimePlan Software A/S’ assertion in section 2 and the related description of the system in section 3 of general IT controls related to the support and development services performed throughout the period from 1 January 2019 to 31 December 2019 (“the description”), and on the design and operation of controls related to the control objectives stated in the description.

This report does not cover general IT controls that are carried out by TimePlan A/S’ sub-service providers 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;
- Logical security, including password policy management regarding servers and databases;
- Management of backup of customer environments, including monitoring and restoring;
- Patch management of hosted servers and databases.

We have therefore not assessed whether relevant controls were suitability designed and operated effectively at the sub-service organisations throughout the period from 01 January 2019 to 31 December 2019.

TimePlan Software A/S’ responsibilities

TimePlan Software A/S is responsible for: preparing the description and accompanying assertion in section 2, Timeplan Software A/S’ Assertion*,* including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; stating the control objectives; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Service Auditor’s Independence and Quality Control

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

Deloitte uses ISQC 1 and therefore maintains a comprehensive system for quality management, including documented policies and procedures for complying with the Code of Ethics for Professional Accountants, professional standards and applicable requirements according to the law and other regulations.

Service Auditor's responsibilities

Based on our procedures, our responsibility is to express an opinion on TimePlan Software A/S' description as well as on the design and operation of controls related to the control objectives stated in this description.

We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "*Assurance Reports on Controls at a Service Organization*", issued by the International Auditing and Assurance Standards Board. That standard requires that we comply with ethical requirements and plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at TimePlan Software A/S involves performing procedures to obtain evidence about TimePlan Software A/S' description of its system, and the design and operating effectiveness of controls. The procedures selected depend on the auditor's judgement, including the assessment of the risk that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the design and operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved. An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the 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 we have obtained is sufficient and appropriate to provide a basis for our opinion.

Limitations of controls at a service organisation

TimePlan Software A/S' description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the control of a system that each individual customer may consider important in its 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. Also, the projection of our opinion to future periods' transactions is subject to the risk that changes may occur 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.

Opinion

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

a) The description fairly presents the IT controls regarding the support and development services performed for TimePlan Software A/S' customers as designed and implemented throughout the period from 1 January 2019 to 31 December 2019;

b) The controls related to the control objectives stated in the description were suitably designed and implemented throughout the period from 1 January 2019 to 31 December 2019;

c) The controls tested, which were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period from 1 January 2019 to 31 December 2019.

Description of tests of controls

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

Intended users and purpose

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

Copenhagen, 3 April 2020

Deloitte
Statsautoriseret Revisionspartnerselskab

Thomas Kühn
Partner, State-Authorised Public Accountant

M. Bagger
Michael Bagger
Director, CISA

2. TimePlan Software A/S' Assertion

The accompanying description has been prepared for customers who have used TimePlan Software A/S' services and their auditors, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves, when assessing the risks of material misstatements of customers' financial statements. TimePlan Software A/S confirms that:

a) The accompanying description in section 3 fairly presents the general IT controls related to TimePlan Software A/S' support and development services used by customers throughout the period from 1 January 2019 to 31 December 2019. The criteria used in making this assertion were that the accompanying description:

   i. Presents how the general IT controls were designed and implemented, including:

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

   ii. Includes relevant details of changes to TimePlan Software A/S' system during the period from 1 January 2019 to 31 December 2019.

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

b) The controls related to the control objectives stated in the accompanying description were suitably designed and operated effectively throughout the period from 1 January 2019 to 31 December 2019. The criteria used in making this assertion were that:

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

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

iii. The controls were consistently applied as designed, including that manual controls were applied by individuals who have the appropriate competence and authority, throughout the period from 1 January 2019 to 31 December 2019.

Aalborg, 3 April 2020
TimePlan Software A/S

Rex Archard Clausager
CEO

3. TimePlan Software A/S’ system description

3.1 Overview

The purpose of this description is to inform the customers of TimePlan Software A/S and their auditors of the systems in place at TimePlan Software A/S and to ensure that the requirements of International Standard on Assurance Engagements (ISAE) 3402, “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 and attendance, and HR administration.

The company was founded in Aalborg in 1990, and today it has 37 dedicated employees. In addition, TimePlan Software A/S have 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 700 companies use TimePlan in over 25 countries from all types of industries in local languages, complying with the collective agreements and labour regulations.

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

Thanks to the continuous and innovative development of the software and the close collaboration with the company's customers through the past 25 years, TimePlan continues to set the standard in the market for an increasing number of industries. TimePlan Software A/S is receptive to the wishes and needs of its customers when it comes to development and implementation of new functionalities. 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 solution are always launched and operated in accordance with the rules and developments in the market, most recently the European General Data Protection Regulation (GDPR) and the annual leave regulations applicable in the Nordic countries.

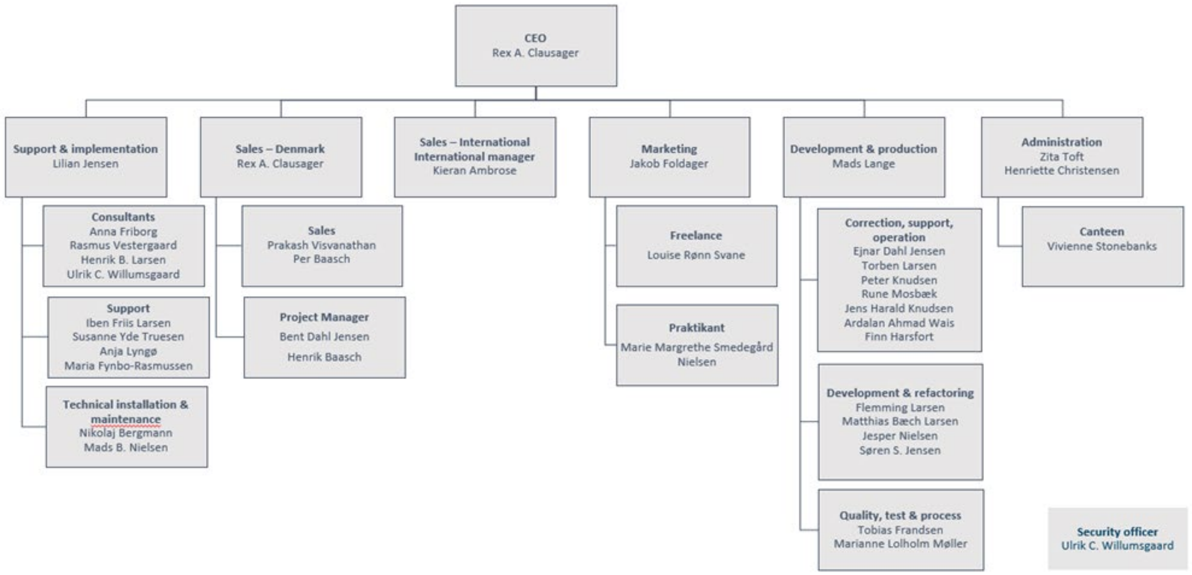
For the past 15 years, TimePlan Software A/S has been AAA accredited in terms of its credit worthiness and is among only 120 companies in Denmark that are AAA Platinum accredited. In 2019, the company was voted no. 14 on Computerworld's software list of leading IT companies in Denmark.

TimePlan Software A/S' core values are:
- Persistence
- Tolerance
- Honesty
- Communication
- Knowledge.

TimePlan Software A/S’ core services are:
- TimePlan
- Software updates

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

3.3. Organisational structure



Organisation chart for TimePlan Software A/S as of 1 October 2019:

3.4 Risk management at TimePlan Software A/S

TimePlan Software A/S uses a risk management system that identifies, analyses and manages 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 objective 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 performance of procedures is obtained throughout the organisation. The process is facilitated by an IT Administrator together with the Information Security Officer, who drafts procedures for the 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 forms part of all service level agreements with third-party service providers. In connection with major projects, depending on the extent and severity, safety assessments and risk management are based on ISO27001 best practices. At an 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 appointed project manager, but it also involves the project participants and the steering group.

3.4.2 Risk management control

TimePlan Software A/S conducts an annual risk analysis complemented by a review of the 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' Security Policy. The Security Policy covers all systems and services offered to customers and is subject to ongoing audit.

3.4.3 Recurring 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 an ISAE 3402 audit.

3.5 Control framework

TimePlan Software A/S' information security policy includes all procedures and processes specified in the TimePlan programme 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 does 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 and A.6 Information security policy and Organisation of information security
- 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 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' Information Security Policy is based on our ISMS and is thus subject to TimePlan Software A/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 is agreed to ensure continued stability, precision and efficiency.

The Information Security Officer (see 3.6.2) 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 which 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 to it.

3.6.2 A.6 Organisation of information security

TimePlan Software A/S has established an internal organisation responsible for managing and implementing information security. This includes communicating with authorities as well as policies on internal and external information security. The Management has appointed an Information Security Officer, who manages tasks that fall under ISMS in collaboration with the Management.

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

Based on the input from internal and external parties, such as the Danish Chamber of Commerce, the Danish Data Protection Agency, legal advisers and internal developers, potential actions of the Information Security Officer are collected and integrated into actual proposals.

3.6.3 A.7 HR and employee security

TimePlan Software A/S' requirements for compliance with information security and confidentiality include employee screening (including criminal records 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 receive official security approval by the relevant authorities.

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

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

The employees of TimePlan Software A/S are regularly informed of IT security awareness matters, and how confidential and personal data should be processed. The Management presents all employees with the Information Security Policy. If an employee violates TimePlan Software A/S’ internal guidelines, the Management can decide to use disciplinary sanctions.

When it comes to termination of an employment relationship, the employee's rights and access are removed, and all company property is to be returned. The employee is then reminded that they are still subject to confidentiality upon termination of employment.

3.6.4 A.9 Access control

TimePlan Software A/S' employees are informed of their responsibilities, and applicable confidentiality 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 data. Standards and control frameworks from ISO27001 are used as a basis for all data and system access policies. This is to ensure a uniform 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.

3.6.4.1 Internal access

It is TimePlan Software A/S' policy that employees should have easy and secure access to 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 the AD with Group Policies has been set to control access and security. Rights are allocated in relation to the position and work function assessed by the individual Department Manager. Rights allocation is verified on an ongoing basis. Rights are assigned or restricted according to the needs defined and maintained by the Department Manager and executed by the IT Administrator.

The IT Administrator is the only person who is authorised 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 change of 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 the rights differ from normal restrictions.

TimePlan Software A/S has described and incorporated a password policy that defines the framework for authentication on all platforms. Passwords will expire within a system-defined timeframe and a corresponding set of rules for the quality of authentication. In addition, centrally controlled deletion rights have been set up. All passwords are encrypted and centrally controlled through an AD-integrated password manager; all passwords are personal; and access is granted on a strict “need to have” basis.

3.6.4.2 External access to network (guests and consultants)

External access for guests is managed on a separate network from TimePlan Software A/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 denied to outsiders. Wi-Fi networks can be accessed in DMZ and are secluded for access to internal systems. Mobile devices, other than PC equipment, grant access to the separate network. There are defined system processes in place to ensure that mobile devices do not access the system network.

3.6.4.3 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 a Data Controller, with TimePlan Software A/S being considered a 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 relation to the organisation's own business. TimePlan's support access and actions are logged directly in the customer's 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/anonymised, so that it is not possible to read or derive personal or company-recordable data. This is only done in agreement with the customer.

3.6.6.4 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' Control Measures Policy (especially Section 6.4). The rules are stated 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. It logs each supporter's connection and access, which is then archived.

3.6.5 A.10 Cryptography

Cryptography is an important tool for TimePlan Software A/S' Information Security Policy. Cryptography is used to secure sensitive, stored data and is used in many places in TimePlan, so that customers can better secure their systems (e.g. by 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 personal data legal obligations in particular. Encryption is used, where data can be considered confidential or personally sensitive in the administration of TimePlan, and protection can be applied on selected fields within the software, where relevant.

3.6.6 A.11 Physical security and environmental protection

3.6.6.1 Local physical security

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

All TimePlan computers must be locked when unattended; this is further enforced through an AD policy that locks computers after five minutes of inactivity. All employee desks must be cleared at the end of each workday to minimise the risk of leaving sensitive information unsecured.

According to TimePlan Software A/S' procedure for Removable Devices and Drives (phones, USB drives), external equipment cannot be connected without documented acceptance by the IT Administrator. Mobile devices are excluded from internal connection; drives are being scanned for malware; and USB keys should be encrypted with, for example, BitLocker if they transport confidential material. TimePlan Software A/S' employees are required to store all critical data on local TimePlan Software A/S servers, which are regularly backed up in accordance with applicable procedures.

Designated employees have keys provided by the 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' on arrival at 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 adjusted by a cooling system.

3.6.6.2 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 with the legal requirements for the processing 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 reviews the supplier service once a year, 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 auditor’s report. Should the documentation be incorrect, the supplier’s contract must be terminated.

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

3.6.6.3 Control of assets

The physical and digital assets of TimePlan Software A/S involved in the provision of services are identified, registered and assigned to an owner. The information is classified in accordance with applicable legal requirements, the value of the information and the sensitive information in relation to unauthorised access or changes. Removable media, such as back-up 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 organisation, all hardware and software is monitored through centralised software, which is reviewed on a monthly basis at a minimum. 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 for proactive action.

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

3.6.7 A.12 Operational security

3.6.7.1 Tools and environment

TimePlan Software A/S' policy on Software Tools and Environment is to run the latest versions to ensure compatibility and security, where possible. The Management must approve all third-party software before it can be installed. The responsibility for software and licences lies with the Management, which can delegate this responsibility to the system owners. The Department Manager and the IT Administrator review the software list annually.

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. Unauthorised software will be uninstalled.

Centralised management of anti-malware software has been set up that ensures latest versions, a unified policy and scan rate. GPO policies have been established to ensure optimal operation, maintenance and uniformity of 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, with emphasis on optimal operation and value. The Management together with the IT Administrator and possibly a third-party provider decide how changes are to be implemented and tested. The IT Administrator maintains the documentation.

Networks are segregated. 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 to 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 may affect customers' operating environments, the customers receive a notification by email within a reasonable timeframe for the contact(s) that the customers have informed TimePlan Software A/S thereof. TimePlan Software A/S also communicates essential service releases and software news.

3.6.7.2 Development

The development environment at TimePlan Software A/S complies with the general policies in section 6.7.1, 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. Please see section 6.9 for a further description.

On an operational level, the environment is secured by way of storage of the code in a version control system, a regular code and environment backups, as well as off-site depositing of a complete copy.

3.6.7.3 Software test

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

3.6.7.4 Operation

The basis for the 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 smallest extent possible.

3.6.7.5 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' standards for secure hosting of software and that such compliance is documented.

Backups and snapshots are taken continuously to ensure continuous operation and an ability to re-establish operations quickly. It is checked and ensured that the backup is generated flawlessly, and any errors are assessed and followed up on. Back-up procedures are described and form an important part of the daily operations. The back-up 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 a basis for the contingency plan. Any necessary fixes and enhancements are versioned into the contingency plan and back-up descriptions. The IT Administrator carries out maintenance and testing, and corrections are made in collaboration with the Department Managers.

3.6.8 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 safely use and access the communication opportunities provided by the platform. Therefore, secure means of communication are always available, when integrated with other systems, and all development procedures require that only secure communications protocols be 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.

3.6.9. 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 perceive as being in sync with the latest trends within development and security that also complies with the current legal and collective requirements.

All development activities are documented in the recording system, where employees document all tasks in the development process on a given case. Code changes are not released until they have been reviewed by a secondary developer and have undergone the nightly regression tests. Furthermore, no releases of new versions are performed until all changes have undergone manual testing by an external test team.

All releases are documented in the workflow management system (WSM) and contain documentation for all issues in the release. Any errors identified in a release candidate, whether identified in manual or automatic tests, must be added to the release issue in the WSM and be resolved prior to release. For main releases, performance tests and release KPIs are created to track performance and ensure that all issues that may have arisen during the release flow have been resolved.

Developments, fixes, improvements and changes occur according to documented workflows, where components are not released until a description, clarification, encoding, code review and system flow tests have been made. In the recording 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 a code for release without involving other developers in the approval process.

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.

3.6.10 A.15 Supplier relationships

Before establishing a work 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 organisation's obligations to the customers. If this is not the case, an alternative must be found. The IT Administrator and the Information Security Officer carry out this review. If a cooperation agreement is made, a Data Processing Agreement will be prepared.

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

Likewise, 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 complementing information security.

3.6.11 A.16 Information security incident management

TimePlan Software A/S is committed to preventing unauthorised access to TimePlan Software A/S' and the 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 contacted to follow up 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 generate an internal incident report that will reduce the likelihood and impact of future events and, if possible, optimise the handling of such events.

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

Any information security weaknesses detected are reported internally and prioritised immediately.

3.6.11.1 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 in 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 GDPR.

3.6.11.2 Accidental exposure in Timeplan

If a version of TimePlan or insecure behaviour in TimePlan Software A/S causes unintended exposure of information, TimePlan Software A/S will process this in accordance with its crisis management procedures. TimePlan Software A/S is committed to helping customers prevent and resolve breaches of information security by, amongst other means, training and delivering best practices to the proper management of the users within TimePlan.

In TimePlan, it is possible to hide, restrict or divulge information that the individual does not need for their daily tasks. In the programme setup, it is easy to incorporate rights profiles, access levels and views.

3.6.12 A.17 Information security aspects of business continuity management

TimePlan Software A/S is committed to addressing all potential threats through a policy on prevention and resolution if a threat is considered serious and/or likely to occur. 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 changes.

At TimePlan Software A/S, there is a contingency plan in place in case of a breakdown. The contingency plan forms the basis of reinstatements or the like and provides a framework for contact and action. The elements of 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.

3.6.12.1 Internal crisis

In case of an internal crisis, such as server loss, TimePlan Software A/S will initiate emergency procedures to minimise 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.

3.6.12.2 Customer crisis

In case of a customer crisis, such as data loss, TimePlan Software A/S will assist the customer with the re-establishment. Individual SLAs can define a framework for crisis management, and, if so, this will form the basis for crisis management. TimePlan Software A/S has standardised 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 form part of ongoing emergency testing.

3.6.12.3 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. Alternatively, the operational environment of a given provider can be moved or re-established. The re-installation is tested at the supplier on an annual basis.

3.6.13 A.18 Compliance

TimePlan Software A/S conducts an annual review of internal procedures, with the Management assessing whether information security is implemented and reviewing the effectiveness of the procedures. There is also a technical compliance review in place to ensure that the TimePlan system is compliant 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. The customers and their auditors should themselves assess whether it is necessary to test integrations or special setups 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 of the financial statements.

Sub-service organisation auditor's reports
As part of the control environment for hosted clients outsourced to the sub-service organisation, the customers with a hosted TimePlan solution should obtain and review the auditor's reports issued by 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 report is intended to provide customers with information about the controls at TimePlan Software A/S that may affect the processing of user organisations’ transactions and also to provide customers with information about the operating effectiveness of the controls that were tested.

This section, when combined with an understanding and assessment of the controls involved in the customers’ business processes, is intended to assist the customers' auditors in (1) planning the audit of the financial statements and in (2) assessing the risk of misstatements of the customers’ financial statements that may be affected by controls at TimePlan Software A/S.

Our testing of TimePlan Software A/S’ controls was restricted to the control objectives and related controls listed in the test table below and was not extended to 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’ customers are not covered by our report. It is assumed that the latter controls are examined and assessed by the customers’ auditors.

This report does not cover any controls performed by the sub-service providers Itadel A/S and Mitcom A/S, as this is the responsibility of the hosting provider as 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 minimise 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 Test of Controls

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

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

4.3 Test of operating effectiveness

Our testing of the control environment involved interviewing relevant Management members, supervisors and employees as well as examining TimePlan Software A/S’ documents. The control environment was assessed in order to determine the nature, timing and scope of controls, and the design and implementation of those controls.

Our test of the operating effectiveness of controls includes such tests as we consider necessary to evaluate whether those controls performed, and the extent of compliance with them, were sufficient to provide reasonable, but not absolute, assurance that the specific control objectives were achieved throughout the period from 1 January 2019 to 31 December 2019.

Our test of the operating effectiveness of controls was designed to cover a representative number of transactions throughout the period from 1 January 2019 to 31 December 2019 for each of the controls listed in this section, which are designed to achieve the specific control objectives.

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.			
5.1.1 *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 the Management. Deloitte has checked by way of inspection 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.
5.1.2 *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 the Management.	Based on interviews and documentation, Deloitte has assessed that there is a procedure in place for reviewing the IT security policy yearly.	No deviations noted.

A.7 Human resource security

A.7.1 Prior to employment

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			
7.1.1 *Screening*	All applicants are screened according to defined screening criteria and relevant laws. For all hires, criminal records are obtained and archived in the employee master record in TimePlan according to the procedure.	Deloitte has observed that a screening procedure is in place describing how the background check is performed. Deloitte has checked by way of inspection for one sample that a criminal record was collected and uploaded to the employee's master record in TimePlan.	No deviations noted.
7.1.2 *Terms and conditions of employment*	For all new hires, an employment contract is made between TimePlan Software A/S and the employee stating the terms and conditions of employment. The employment contract contains a confidentiality agreement.	Deloitte has observed that a procedure for setting terms and conditions is in place specifying that contracts must be in place for all new employees. Deloitte has checked by way of inspection on a sample basis that a contract for employment is made covering the terms and conditions of employment, and that a confidentiality agreement has been signed.	No deviations noted.

A.7.2 During employment

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			
7.2.1 *Management responsibilities*	Department Managers have the responsibility to ensure compliance with the IT security policy, as well as policies relevant to their department. Furthermore, the Management has appointed an IT security responsible.	Deloitte has observed that a policy stating the Management's responsibility for compliance with procedures is in place. Deloitte has checked by way of inspection that roles are defined on the organisational chart, and that an IT security responsible has been appointed.	No deviations noted.
7.2.2 *Information security awareness, education and training*	The Management of TimePlan Software A/S 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 by email.	Deloitte has observed that a procedure regarding information security awareness and training is in place. Deloitte has inquired whether IT security awareness training is performed on a periodic basis and inspected a sample of awareness emails.	No deviations noted.

A.9 Access control

A.9.2 User access management

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services			
9.2.1 *User registration and de-registration*	User administration procedures have been prepared, and a Department Manager must initiate all internal user registrations or de-registrations. If an employee is terminated, the user profile is deleted when the employee leaves the company. The Management initiates the removal of rights through Jira, and, based on this, system access is revoked by the IT Administrator.	Deloitte has observed that a procedure for registering and de-registering users is in place. Based on a sample, Deloitte has assessed if the user registration and de-registration is initiated by a Department Manager. Deloitte has observed that a procedure for removing access rights is in place. Deloitte has tested a sample of terminated users and verified that the corresponding user profile and access have been revoked.	No deviations noted.
9.2.3 *Management of privileged access rights*	Only a few selected users have administrative rights for 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 managing privileged access rights is in place and has reviewed the list of employees with privileged access rights. Deloitte has reviewed all users with administrative rights on the TimePlan Software A/S domain and TimePlan Software A/S' managed admin users on hosted domains, and verified them with the Management.	We noted that one user has access to all internal environments and the corresponding infrastructure internally at TimePlan Software A/S. Further, we have noted that developers use a shared 'sa' account on one of the hosted domains.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
9.2.4 *Management of secret authentication information for users*	TimePlan Software A/S has created a password policy covering the internal domain in which 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 reviewed the implemented password policy on the internal TimePlan Software A/S domain and assessed whether it complies with the baselines and security standards defined.	We noted that the password policy did not follow the baselines and security standards, as lockout settings are not applied. However, we have checked by way of inspection that the security parameters regarding passwords have been improved as a result of the audit. No further deviations noted.
9.2.5 *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 periodically reviewing 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.	We noted that a procedure for periodically reviewing access rights is in place, but that no documentation supporting the performance of the access review is available.

A.9.4 System and application access control

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent unauthorised access to the system			
9.4.2 *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 secure login procedure is in place. Deloitte has observed that access on the TimePlan Software A/S internal domain is governed by passwords, and we have observed on a sample basis that access from the external network is validated through VPN.	No deviations noted.
9.4.3 *Password management system*	TimePlan Software A/S has established a procedure defining the 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 password management procedure is in place. Deloitte has inquired with key personnel and verified the storage procedures for standard passwords.	No deviations noted.
9.4.4 *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. A TimePlan Software A/S employee must obtain a formal approval from the customer before accessing the customer environment. Any 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 to customer environments. Based on a sample, Deloitte has checked by way of inspection that a customer approval was in place for granting access to a customer environment.	No deviations noted.

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.			
10.1.1 *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 that the TimePlan software uses for cryptography and the encryption programs that the employees are allowed to use.	Deloitte has observed that an encryption procedure is in place and verified for samples of data extracted from the database that the data in TimePlan was encrypted.	No deviations noted.

A.11 Physical and environmental security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To prevent unauthorised physical access and damage to and interference in the organisation's information and information processing facilities.			
11.2.6 *Security of off-premise equipment and assets*	Home offices for TimePlan Software A/S employees are set up with approval from the CEO.	Deloitte has observed that a policy for securing off-premise equipment and assets is in place, which covers assets at the external hosting companies and assets located at employees' home offices. Based on inquiries with key personnel, we noted that the number of employees with home offices only amounts to one employee. We noted that this was approved by the CEO.	No deviations noted.
11.2.8 *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. Further, we have observed that a mobile device password policy is in place.	No deviations noted.
11.2.9 *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 checked by way of inspection selected departments at TimePlan Software A/S' location and noted that unmanned desks were cleared.	No deviations noted.

A.12 Operations security

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure correct and secure operation of information processing facilities.			
12.1.1 *Written guidelines and procedures*	Based on ISO27001, TimePlan Software A/S has defined written guidelines and procedures, and these procedures are available to all employees on the intranet.	Deloitte has checked by way of review that procedures are stored on the intranet and made available to TimePlan Software A/S' employees.	No deviations noted.
Control objective: To ensure that information and information processing facilities are protected against malware.			
12.2.1 *Controls against malware*	TimePlan Software A/S has installed anti-virus 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 protecting against malware is in place, and that it requires anti-virus software to be installed on all clients and servers internally. Deloitte has checked by way of inspection for one sample of clients and servers that anti-virus protection is installed, and that definitions are updated.	No deviations noted.
Control objective: To protect against loss of data.			
12.3.1 *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, they are handled by the IT Administrator in collaboration with the hosting partner.	Deloitte has observed that a back-up procedure is in place. Deloitte has obtained documentation for the back-up strategy and verified the back-up configuration. Deloitte has checked by way of inspection one sample of back-up jobs and verified that the back-up jobs ran successfully.	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To record events and generate evidence.			
12.4.1 *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 through Remote Desktop. In case of security violations and unauthorised 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 deviations noted.
12.4.2 *Protection of log information*	All logs are sent to the log management tool through 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 in place, we have checked by way of inspection if the log setup is appropriate.	No deviations noted.
Control objective: To prevent exploitation of technical vulnerabilities.			
12.6.1 *Management of technical vulnerabilities*	All equipment is continuously monitored by 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 managing technical vulnerabilities is in place. For a sample of servers, Deloitte has checked by way of inspection that the servers were patched appropriately.	No deviations noted.

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.			
13.1.1 *Network controls*	Internal networks used in TimePlan Software A/S are closed and secured against unauthorised access. All access to network equipment is password protected, and admin access is restricted to a few persons. All network access in TimePlan Software A/S is logged.	Deloitte has observed that a procedure governing network controls is in place, and that the procedure contains rules on network access. Deloitte has inspected the high-level network security and noted that a password is required to gain access. Further, we noted during the inspection that traffic is logged, and that privileged access is limited to a few authorised employees.	No deviations noted.
13.1.3 *Segregation in networks*	TimePlan Software A/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.

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 life cycle. This also includes requirements for information systems which provide services over public networks.			
14.1.1 *Information security requirements analysis and specification*	TimePlan Software A/S has defined information security requirements as 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 has tested one sample of changes to verify that security requirements were specified and documented in the Jira flow.	We noted that the formal registration of the security risk assessment for changes is not always documented in Jira.
Control objective: To ensure that information security is designed and implemented within the development life cycle of information systems.			
14.2.1 *Secure development policy*	TimePlan Software A/S has defined change management procedures regarding secure development, build and deployment processes.	Deloitte has observed that change management procedures are in place, and that they cover considerations regarding secure development.	No deviations noted.
14.2.2 *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 of changes that the change management flow was adequately followed and documented.	No deviations noted.
14.2.3 *Technical review of applications after operating platform changes*	TimePlan Software A/S performs a code and design review on all changes before releasing a build. A release document is signed by the Management before the version is released to the customers.	Deloitte has verified that the procedure for reviewing systems after changes is in place. Deloitte has verified for one sample of changes that a code and design review was performed, and that a release document was made and signed for the selected release.	No deviations noted.
14.2.6 *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 guidelines on secure development environments are in place. Deloitte has obtained documentation regarding the segregation of development,	No deviations noted.

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
		test and operating environments, and assessed that the environments are physically segregated.	
14.2.8 *System security testing*	A test of security functionality is carried out as 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 testing system security is in place. The procedure also includes security considerations in the review phases. Deloitte has verified for one sample of changes that design review, code review and integration testing were performed.	We noted that it was possible to have the same person responsible for both design review, code review and integration testing; hence the system security procedure has not been fully implemented. We were informed that the procedure has been rectified as a result of the audit. No further deviations noted.
14.2.9 *System acceptance testing*	TimePlan Software A/S has defined guidelines for testing the developed solutions. All functionalities are tested manually and approved before the functionality is subjected to automated, nightly integration tests. No functionality with errors will be approved for final release.	Deloitte has observed that a procedure governing system acceptance testing is in place. Deloitte has verified for one sample of changes 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 objective: To ensure the protection of test data.			
14.3.1 *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 anonymised/scrambled on the test database.	Deloitte has observed that a procedure for protecting test data is in place. Deloitte has for one sample of test data checked by way of inspection that test data was scrambled on the test database.	No deviations noted.

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.			
15.1.1 *Information security policy for supplier relationships*	TimePlan Software A/S periodically assesses if the supplier is able to comply with information security guidelines consistent with those set by TimePlan Software A/S.	Deloitte has observed that a procedure regarding information security requirements for suppliers is in place. Deloitte has checked by way of inspection that a data processing agreement has been signed by TimePlan Software A/S and the suppliers Itadel A/S and Mitcom A/S.	No deviations noted.
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
15.2.1 *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 agreed services were delivered, and that the established information security requirements are complied with.	Deloitte has observed that a procedure for monitoring and reviewing 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 quarterly reports of the delivered services received from a supplier.	No deviations noted.

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.			
16.1.1 *Responsibilities and procedures*	TimePlan Software A/S has prepared a procedure for handling information security events that defines responsibilities.	Deloitte has reviewed the procedure for handling information security events and obtained the organisational chart in which the corresponding responsibilities are stated.	No deviations noted.
16.1.3 *Reporting information security weaknesses*	Information security weaknesses will be reported to the Management and the IT security responsible through Jira, and a case will be documented through there.	Deloitte has observed that a procedure for reporting information security weaknesses is in place, and that it covers appropriate reporting.	We were informed that no security weaknesses to be reported were detected during the audit period.

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.			
17.1.1 *Planning information security*	TimePlan Software A/S has prepared a disaster recovery plan that 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. 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 inspected the disaster recovery plan and assessed its contents in terms of TimePlan Software A/S' internal organisation and setup. Deloitte has inspected the documentation describing the disaster recovery scenarios, which covers internal crises, customer crises and crises at hosting suppliers.	No deviations noted.
17.1.3 *Verify, review and evaluate information security continuity*	TimePlan Software A/S performs periodic testing of relevant disaster recovery scenarios, as well as manual simulations of events.	Deloitte has observed that the disaster recovery plan contains relevant scenarios. Deloitte has checked by way of inspection that disaster recovery scenarios have been tested within TimePlan Software A/S' internal organisation.	No deviations noted.

A.18 Compliance

Control Activity	Client Control Activity	Audit Procedures Performed	Test Results
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures.			
18.2.2 *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 person responsible reviews the procedures.	Deloitte has observed that a procedure for complying with security policies and standards is in place, and that responsibilities and the scope of review of procedures are defined.	No deviations noted.
18.2.3 *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.