Assurance report

TimeLog A/S

ISAE 3402 type 2 assurance report on IT general controls for
the period 13 April 2021 to 31 July 2022 related to SaaS services

December 2022

Grant Thornton | www.grantthornton.dk
Højbro Plads 10, 1200 København K
CVR: 34 20 99 36 | Tel. +45 33 110 220 | mail@dk.gt.com

Table of contents

Section 1: Description of TimeLog A/S' services in connection with the operating of SaaS services

1.1. Description of TimeLog A/S' services in connection with SaaS services

The following is a description of TimeLog A/S' services which are included in the IT general controls of this assurance report. The report includes general processes and system setups etcetera with TimeLog A/S. Processes and system setups etcetera, individually agreed with TimeLog A/S' customers, are not included in this report. Assessment of customer specific processes and system setups etcetera will be stated in specific assurance reports for customers who may have ordered such.

Controls in the application systems are not included in this report.

1.2. IT general controls at TimeLog A/S

Introduction

In the following, a description of the general IT controls related to TimeLog A/S' services to customers, according to the above description in paragraph 1.1., will be provided.

The purpose of the following report is to provide TimeLog A/S' customers and their auditors with information regarding the requirements of ISAE 3402, which is the international auditing standard for assurance reports on controls at service organisations. In the following, a description of the general information security controls related to TimeLog's services to customers, will be provided.

The scope of the following description is exposure of the technical and organisational security measures which have been implemented in connection with the operation of TimeLog. We have reviewed all the commonly accepted information security controls specified in ISO 27002:2017. TimeLog has assessed its compliance with these controls as stated under each control.

TimeLog and our services

TimeLog is a market leading Professional Services Automation (PSA) software, targeting consulting and advisory companies who aim high and have the ambition to develop their business and optimise internal workflows all the way from the initial contract to the final invoice. For more than 20 years, TimeLog has grown and today it has offices in Denmark (HQ), Sweden and Malaysia.

Our services cover time tracking, project management, automated project invoicing, resource management, invoicing and finances, customer management, reporting, integrations, HR, and employee management.

Use of subservice organisations

TimeLog uses GlobalConnect A/S as subcontractor of physical security in data centres. GlobalConnect is responsible for physical security, hardware, networking, backup, and storage. This report has been prepared according to the "exclusive method," and thus, it does not include controls of GlobalConnect. GlobalConnect's ISAE 3402-II report for 2021 can be received upon request from GlobalConnect.

Risk assessment and management

The risk assessment is conducted to document TimeLog's risk-based approach for selecting security measures and provides an assessment of all identified risks. The purpose of the risk assessment is to ensure that the procedure and implemented security measures match the risk that occur, both when internal and external factors are taken into consideration.

The steps and methodology of the risk assessment follow the process which is considered part of the ISO/IEC security standard. The residual risk is assessed based on the risk image and the implemented security measures. In this way it is assessed whether the implemented security measures are adequate or if further action should be taken.

The risk assessment is updated at least once a year and otherwise when it is relevant. The responsibility for the risk assessment lies with the CEO of TimeLog, who also approves the assessment.

Organisation of information security

In order to establish, implement, maintain, and improve TimeLog's Information Security policy, TimeLog uses the international standards of ISO/IEC 27002. TimeLog reviews all the commonly accepted information security controls specified in ISO 27002:2017 which applies to all employees and deliveries.

The methodology for the implementation of controls is divided into the following control areas:

A.5 Information security policies

A.6 Organisation of information security

A.7 Human resource security

A.8 Asset management

A.9 Access control

A.10 Cryptography

A.11 Physical and environmental security

A.12 Operations security

A.13 Communications security

A.14 Acquisition, development, and maintenance of systems

A.15 Supplier relationships

A.16 Information security incident management

A. 17 Information security aspects of business continuity management

A. 18 Compliance

Management of information security within the individual areas, are described below. Control objectives and controls, chosen by TimeLog, are also stated in the summary in section 4.

A.5 Information security policies

A.5.1.1 Policies for information security

Our information security policy creates the framework for an operational management system which implements guidelines on how to handle information security in TimeLog. Responsibility placement, guidelines, risk management and IT contingency plans are therefore topics that are regulated under this management system.

The information security policy covers all our activities, including development, delivery, and services to TimeLog customers. The information security policy is based on generally accepted methods and policies for information security, including best practice in complying with the principles described in the international ISO/IEC 27002 standard. Furthermore, the policy is based on relevant rules, legal requirements, and guidelines within TimeLog's business area.

A.5.1.2. Review of policies for information security

TimeLog's information security policy is reviewed regularly and approved by the management once a year. TimeLog aims at continuously improving both policies, procedures, and operations.

A.6 Organisation of information security

A.6.1 Internal organisation

A.6.1.1 Information security roles and responsibilities

TimeLog has defined and allocated all information security responsibilities.

A.6.1.2 Segmentation of duties

Conflicting duties and areas of responsibility have been segregated within TimeLog to reduce the opportunities for unauthorized or unintentional modification or misuse of the organisation's assets. Furthermore, the role of the system administrator and regular users are defined in all relevant systems.

A.6.1.3 Contact with authorities

TimeLog has procedures in place that specify when and by whom authorities should be contacted, and how identified information security incidents should be reported in a timely manner.

A.6.2 Mobile devices and teleworking

A.6.2.1 Mobile device policy

All TimeLog employees with a company smartphone are required to install Microsoft Endpoint Company Portal on their device.

A.6.2.2 Teleworking

Access to our network, systems and data is only possible for authorized persons. Furthermore, TimeLog has two types of VPN connections and access to servers and desktops are gained with RDP.

A.7 Human resource security

Human resource security requires measures to reduce the risk of human error, fraudulent conduct or similar.

A.7.1 Prior to employment

A.7.1.1 Screening

TimeLog has a recruitment process with relevant stages for each recruitment. TimeLog uses Teamtailor to make sure that each candidate is evaluated correctly, and that skills and background matches the company's needs for the specific position.

A.7.1.2 Terms and conditions of employment

General terms of employment, as well as confidentiality is specified in each employment contract.

A.7.2 During employment

A.7.2.1 Management responsibility

All TimeLog employees and contractors are required to apply information security in accordance with established policies and procedures. This is also stated in TimeLog's employee handbook and information security policy which is accessible to all employees. Furthermore, an NDA is to be signed prior to commencing work.

A.7.2.2 Information security awareness education and training

During the first weeks of employment, head of HR arranges onboarding meetings with new employees where relevant topics related to their job description is carried out. All employees receive a general appropriate introduction on how TimeLog works with information security, and everyone has access to the organisation's information security policy.

It is mandatory for all TimeLog employees to complete awareness training courses which are assigned every second month. The topics vary each time, with focus on relevant issues related to information security and data protection.

A.7.2.3 Disciplinary process

All employment contracts contain general terms of employment, as well as confidentiality. Penalties following breaches is furthermore stated.

A.7.3 Termination and change of employment

A.7.3.1 Termination or change of employment responsibilities

In case of termination, a procedure will be initiated to ensure that the employee returns all relevant assets, such as portable devices, and that all access to system, data and offices is withdrawn. Head of HR and the relevant line manager go through a checklist prior to termination. The documentation related to the termination of employment is available electronically in our recruitment system, Typelane.

A.8 Asset management

The objective of this section is to identify TimeLog's assets and define appropriate protection responsibilities.

A.8.1 Responsibility for assets

A.8.1.1 Inventory of assets

TimeLog is maintaining records of assets associated with information and information processing facilities.

A.8.1.2 Ownership of assets

TimeLog has assigned ownership of its assets to relevant staff and GlobalConnect.

A.8.1.3 Acceptable use of assets

TimeLog's Employee Handbook and Information Security Policy cover this area.

A.8.1.4 Return of assets

TimeLog has formalized the termination process to ensure that all relevant organisation assets in the possession of the employee are returned upon termination of their employment. Furthermore, all access rights to systems and buildings are taken away.

A.8.3 Media management

A.8.3.2 Disposal of media

TimeLog has an established procedure for disposal of media for portable devices, including personal computers, USB sticks etc.

A.8.3.3 Transport of physical media

TimeLog has implemented appropriate procedures to protect media containing information against unauthorized access, misuse, or corruption during transportation. TimeLog ensures that all laptops are governed by Microsoft Intune and Bitlocker encrypted.

A.9 Access control

The objective of this section is to limit access to information and information processing facilities. TimeLog allocates access rights based on work related needs, considering efficient segmentation of duties.

A.9.1 Business requirements of access control

A.9.1.1 Access control policy

TimeLog has established an access control policy, which is reviewed based on business and information security requirements. On a per system basis, the system owner assigns appropriate roles of access.

A.9.1.2 Access to network and network services

TimeLog has a policy concerning the use of networks and network services to ensure that users are only provided with access to the network and network services that they have been specifically authorized to use. Company networks are separated physically and/or logically to ensure the correct authorized use.

A.9.2 User access management

The objective is to ensure authorized user access and to prevent unauthorized access to systems and services.

A.9.2.1 User registration and de-registration

TimeLog has implemented user registration and de-registration process to enable assignment of access right. This process is activated during on/off-boarding and when employees change position and responsibilities within TimeLog.

A.9.2.2 User access provisioning

TimeLog has implemented user access provisioning process to assign or revoke access right for all user types, to all systems and services which is handled on a system-by-system basis by the relevant system owner.

A.9.2.3 Management of privileged access rights

TimeLog controls the allocation of privileged access rights through authorization process in accordance with relevant access policy. Furthermore, TimeLog has peer-approval on Microsoft 365 services.

A.9.2.4 Management of secret authentication information of users

TimeLog controls the allocation of secret authentication information through a formal management process. For systems supporting initial one-time passwords, TimeLog never distributes secret authentication information.

A.9.2.5 Review of user access rights

TimeLog's asset owners review user access rights at regular intervals, and as minimum, twice a year.

A.9.2.6 Removal or adjustment of access rights

TimeLog follows procedures to ensure that access right of all employees and external parties to information and information processing facilities are removed upon termination of their employment, contract, or agreement, or adjusted upon change.

A.9.3 User responsibilities

A.9.3.1 Use of secret authentication information

All employees at TimeLog are required to follow the company's practices in the use of secret authentication information.

A.9.4 System and application access control

A.9.4.3 Password management system

The password management systems used in TimeLog are interactive. Furthermore, Dashlane has been implemented.

A.10 Cryptography

The objective is to ensure proper and effective use of cryptography to the confidentiality, authenticity and/or integrity of information.

A.10.1 Cryptographic controls

A.10.1.1 Policy on the use of cryptographic controls

TimeLog uses encryption to secure data and communication. On a case-by-case basis, TimeLog identifies risks and determines if encryption is needed, and if needed, how strong an encryption is required to mitigate the risks.

A.10.1.2 Key management

TimeLog has a policy on the use, protection, and lifetime of cryptographic keys on a per system basis which covers SSL and code signing certificates, and login portal signing certificates. Both are renewed annually.

A.12 Operations security

The objective is to ensure correct and secure operations of information processing facilities.

A.12.1 Operational procedures and responsibilities

A.12.1.1 Documented operating procedures

TimeLog has operating procedures that are documented and made available to relevant users who need them due to their work.

A.12.1.2 Change management

TimeLog's development procedure follows a uniform process for all development activities, which has been portrayed for audit. The development process is normally part of the larger Project Process, which safeguards that the right initiatives are launched and includes a high-level Change Management assessment.

A.12.1.3 Capacity management

TimeLog has set up monitoring of capacity with alerts sent to relevant employees for proactive actions on constraints.

A.12.1.4 Separation of development, testing and operational environments

TimeLog separates development, testing and operational environments to reduce the risk of unauthorized access or change to the operational environment. This has been illustrated in a network diagram.

A.12.2 Protection from malware

A.12.2.1 Controls against malware

To ensure that information and information processing facilities are protected against malware, TimeLog has implemented detection, prevention, and recovery controls to protect against malware, including appropriate user awareness.

A.12.3 Backup

A.12.3.1 Backup

In order to protect against loss of data, TimeLog has established a backup policy and provided adequate backup facilities to ensure that all essential information and software can be recovered following a disaster or media failure.

A.12.4 Logging and monitoring

A.12.4.1 Event logging

TimeLog keeps event logs whenever users make changes related to their subscription of TimeLog. The log can be viewed inside the product and is also available for TimeLog employees through TCAM.

A.12.4.2 Protection of log information

Logs are protected against modification and deletion.

A.12.4.3 Administrator- and operator logs

The administrator and operator logs are treated the same. Based on context and requirements, TimeLog logs both in a searchable format.

A.12.4.4 Clock synchronization

The clocks of all relevant information processing systems at TimeLog have been defined and implemented as single reference time source for all relevant information processing systems. Servers synchronize with the domain controller using the NTP protocol.

A.12.6 Technical vulnerability management

A.12.6.1 Management of technical vulnerabilities

TimeLog manages technical vulnerabilities as an ongoing part of the established IT Risk Management process.

A.12.6.2 Restrictions on software installation

TimeLog's office environment is fully segregated from TimeLog operations. Therefore, TimeLog has consciously chosen not to limit its users' capabilities, but rather educate them to follow best practices.

A.13 Communications security

Network security includes requirements for network stability, where data transmissions between TimeLog and customers/partners are protected against unauthorized access and inaccessibility.

A.13.1 Network security management

A.13.1.1 Network controls
TimeLog has implemented controls to ensure the security of information in networks and the protection of connected services from unauthorized access. Furthermore, TimeLog use logically separated networks and established firewalls.

A.13.1.2 Security of network services
TimeLog has identified security mechanisms, service levels and management requirements of all network services. These will be included in network services agreements in the future.

A.13.1.3 Segmentation in networks
TimeLog segregates groups of information services, users and information systems on networks.

A.13.2 Information transfer

A.13.2.1 Information transfer policies and procedures
Formal transfer policy procedures and controls are in place to protect the transfer of information.

A.13.2.3 Electronic messages

TimeLog has identified the requirement for handling electronical messages.

A.13.2.4 Confidentiality or non-disclosure-agreements
TimeLog has identified the requirements for confidentiality or non-disclosure agreements, reflecting TimeLog's need for the protection of information for all parties involved in our business, either through employment contracts or cooperation agreements.

A.14. Acquisition, development, and maintenance of systems

The objective is to ensure that information security is an integral part of information systems across the entire lifecycle.

A.14.2 Security in development and support processes

A.14.2.1 Security development policy
TimeLog has established and applied rules for the development of software and systems to development. R&D, spearheaded by Tech Lead, maintains a portal, (Tech Nirvana) for style guides and manifestos related to the development work. The purpose of Tech Nirvana is to align the development structure and patterns among developers.

A.14.2.2 System change control procedures
TimeLog controls changes to systems within the development cycle using formal change control procedures. TimeLog uses Git(log) and pull request approval process (gate).

A.14.2.3 Technical review of applications after operating platform changes
TimeLog reviews and tests business critical applications to ensure that there is no adverse impact on organisational operations or security when operating platforms are changed.

A.14.2.5 Secure system engineering principles
TimeLog enforces various system engineering principles for ensuring a secure environment. Additionally, TimeLog encourages its teams to continuously improve security in any aspect of the development lifecycle. The DevOps team spearheads this initiative.

A.14.2.6 Secure development environment
TimeLog has established an appropriately protected secure development environments for system development and integration efforts that cover the entire system development lifecycle. Developers work in sandboxed environments on local machines while doing development. Developers have access to a user acceptance test (UAT) server. The UAT server is logically separated from the production servers.

Developers can request to push code to UAT servers using a DevOps pipeline (which can include automated checks and tests). Developers can request to push code to production servers using a pull request. Requests to production environments requires a peer developer to approve and/or a DevOps engineer.

A.14.2.7 Outsourced development
TimeLog supervises and monitors the activity of outsourced system development.

A.14.2.8 System security testing
Quality Assurance (QA) has, or gets from Product Owner (PO), basic understanding of the security requirements for each individual feature development to ensure that the system works as expected and only as expected. QA is responsible for covering system security tests to the best of their abilities with the information given.

A.14.2.9 System acceptance testing
TimeLog has established acceptance testing programs and related criteria for new information systems, upgrades and new versions, where there is a combination of product owner approval and QA approval.

A.14.3 Test data
TimeLog has procedures in place to ensure that test data is carefully selected, protected, and controlled.

A.15 Supplier relationships

This section includes information security requirements, in order to manage risk connected with suppliers and outsourcing partners.

A.15.2 Supplier service delivery management

The objective is to maintain an agreed level of information security and service delivery in line with supplier agreements.

A.15.2.1 Monitoring and review of supplier services
TimeLog reviews the services of its suppliers on an annual basis if it is deemed relevant. The list of suppliers is, in relation to this, reviewed annually to ensure that the need to review is evaluated on an ongoing basis.

A.15.2.2 Changes to supplier services
TimeLog reviews the supplier services and ensures that relevant action is taken to changes in the supplier services.

A.16 Information security incident management

The objective is to ensure a consistent and effective approach to the management of information security incidents, including communication of security events and weaknesses.

A.16.1 Management of information security incidents and improvements

A.16.1.1 Responsibilities and procedures
TimeLog has established management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents. The plan will be maintained at least once a year and approved by management.

A. 16.1.2 Reporting information security events
TimeLog has established and communicated procedures for reporting information security events, including the point of contact to which the event should be reported. All employees are aware of their responsibility to report information security events as quickly as possible. This is communicated during onboarding and regularly emphasized to the organisation.

A.16.1.3 Reporting information security weaknesses
TimeLog has established and communicated process flow to reporting information security weaknesses.

A.16.1.4 Assessment of and decision on information security events
TimeLog assesses each information security event and decides whether the event should be classified as an information security incident.

A.16.1.5 Response to information security incidents
TimeLog has designated the responsibility of responding to information security incidents in accordance with the organisation's procedures on the topic.

A.16.1.6 Learning from information security

TimeLog has established process to ensure root-cause analysis is made in accordance with the organisation's procedures on the topic.

A.17 Information security aspects of business continuity management

This section includes requirements of continuity management, including preparation and test of contingency plans.

A.17.1 Information security continuity

A.17.1.1 Planning information security continuity
TimeLog has prepared a disaster recovery plan which forms the basis for restoring the business-critical systems identified.

A.17.1.2 Implementing information security continuity
TimeLog has together with GlobalConnect a documented process on how to implement and maintain procedures and controls to ensure that the required level of continuity for information security during an adverse situation is handled. This will be tested once a year according to our year wheel.

A.17.1.3 Verify review and evaluate information security continuity
TimeLog schedules one annual review session of the contingency plan. For each iteration, TimeLog makes an internal review and makes appropriate changes. Second, GlobalConnect is informed about the changes and an additional review is done. Changes are posted to TimeLog Tech Nirvana and GlobalConnect's document library for TimeLog.

A.18 Compliance

The objective is to avoid breaches on relevant information security requirements.

18.2 Information security reviews

18.2.1 Independent review of information security
TimeLog's approach to managing information security and its implementation will be reviewed independently at planned intervals, when preparing the annual ISAE 3402 report, and when significant changes occur.

18.2.2 Compliance with internal procedure and policies

TimeLog has established and implemented relevant controls to ensure tasks are performed according to procedures and policies.

18.2.3 Technical compliance review
TimeLog has ensured that technical review is done by relevant employees.

Significant changes in IT environments

During the audit period TimeLog has migrated to new hosting centres at GlobalConnect.

Complementary controls with the customers

TimeLog customers are, unless otherwise agreed, responsible for establishing connection to TimeLog servers. Furthermore, TimeLog customers are, unless otherwise agreed, responsible for:

- Administration and periodical review of own user profiles and system resources
- Own internet connection
- Maintaining traceability in third-party software managed by the customer
- Own data
- Compliance with applicable Service Level Agreement which is available on TimeLog's website
- Correct setup of roles and privileges on the system administration of the product
- Password management of API users related to the TimeLog product

Section 2: TimeLog A/S' statement

The accompanying description has been prepared for customers who have used TimeLog A/S' SaaS services and their auditors who have a sufficient understanding to consider the description along with other information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

TimeLog A/S is using subservice organisation Global Connect A/S. This assurance report is prepared in accordance with the carve-out method and TimeLog A/S' description does not include control objectives and controls within Global Connect A/S.

TimeLog A/S confirms that:

(a) The accompanying description in Section 1 fairly presents the IT general controls related to TimeLog A/S' SaaS services processing customer transactions throughout the period 13 April 2021 to 31 July 2022

The criteria used in making this statement were that the accompanying description:

(i) Presents how the system was designed and implemented, including:
- The type of services provided
- The procedures within both information technology and manual systems, used to manage IT general controls
- Relevant control objectives and controls designed to achieve these 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 us alone
- Other aspects of our control environment, risk assessment process, information system and communication, control activities, and monitoring controls that were relevant to IT general controls

(ii) Contains relevant information about changes in the IT general controls, performed during the period 13 April 2021 to 31 July 2022

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

(b) The controls related to the control objectives stated in the accompanying description were suitably designed and functioning during the period 13 April 2021 to 31 July 2022. The criteria used in making this statement were that:

(i) The risks that threatened achievement of the control objectives stated in the description were identified

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

(iii) The controls were used consistently as drawn up, including the fact that manual controls were performed by people of adequate competence and authorization, during the period from 13 April 2021 to 31 July 2022

Frederiksberg, 9 December 2022
TimeLog A/S

Per-Henrik Nielsen
CEO

Section 3: Independent service auditor's assurance report on the description of controls, their design and functionality

To TimeLog A/S, their customers and their auditors.

Scope

We have been engaged to report on TimeLog A/S' description in Section 1 of its system for delivery of TimeLog A/S' services throughout the period 13 April 2021 to 31 July 2022 (the description) and on the design and operation of controls related to the control objectives stated in the description.

TimeLog A/S is using subservice organisation Global Connect A/S. This assurance report is prepared in accordance with the carve-out method and TimeLog A/S' description does not include control objectives and controls within Global Connect A/S.

Some of the control objectives stated in TimeLog A/S' description in Section 1 of IT general controls, can only be achieved if the complementary controls with the customers have been appropriately designed, and works effectively with the controls of TimeLog A/S. The report does not include the appropriateness of the design and operating effectiveness of these complementary controls.

TimeLog A/S' responsibility

TimeLog A/S is responsible for preparing the description (section 1) and accompanying statement (section 2) including the completeness, accuracy, and method of presentation of the description and statement. Additionally, TimeLog A/S is responsible for providing the services covered by the description; stating the control objectives; and for the design, implementation, and effectiveness of operating controls for achieving the stated control objectives.

Grant Thornton's independence and quality control

We have complied with the independence and other ethical requirements of the International Ethics Standards Board for Accountants' International Code of Ethics for Professional Accountants issued by the International Ethics Standards Board for Accountants (IESBA Code), which is founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour and ethical requirements applicable to Denmark.

Grant Thornton applies International Standard on Quality Control 1[1] and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards, and applicable legal and regulatory requirements.

Grant Thornton's responsibility

Our responsibility is to express an opinion on TimeLog A/S' description (Section 1) as well as on the design and operation of the controls related to the control objectives stated in that description based on our procedures. We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", issued by International Auditing and Assurance Standards Board.

This standard requires that we plan and perform our procedures to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, and the controls are suitably designed and operating effectively.

An assurance engagement to report on the description, design and operating effectiveness of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of its system, and the design and operating effectiveness of controls.

[1] ISQC 1, Quality control for firms that perform audits and reviews of financial statements, and other assurance and related services engagements.

The procedures selected depend on the service auditor's judgement, including the assessment of the risks that the description is not fairly presented, and that controls are not suitably designed or operating effectively. Our procedures included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the control objectives stated in the description were achieved.

An assurance engagement of this type also includes evaluating the overall presentation of the description, the suitability of the objectives stated therein, and the suitability of the criteria specified by the service organisation.

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

TimeLog A/S' description in section 1, 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 systems that each individual customer may consider important in their own particular environment. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Furthermore, the projection of any functionality assessment to future periods is subject to the risk that controls with service provider can be inadequate or fail.

Opinion

Our opinion has been formed based on the matters outlined in this report. The criteria we used in forming our opinion were those described in TimeLog A/S' statement in Section 2 and based on this, it is our opinion that:

(a) The description of the controls, as they were designed and implemented throughout the period 13 April 2021 to 31 July 2022, is fair in all material respects.
(b) The controls related to the control objectives stated in the description were suitably designed throughout the period 13 April 2021 to 31 July 2022 in all material respects.
(c) The controls tested, which were the controls necessary for providing reasonable assurance that the control objectives in the description were achieved in all material respects, have operated effectively throughout the period 13 April 2021 to 31 July 2022.

Description of tests of controls

The specific controls tested, and the nature, timing and results of these tests are listed in the subsequent main section (Section 4) including control objectives, test, and test results.

Intended users and purpose

This assurance report is intended only for customers who have used TimeLog A/S and the auditors of these customers, who have a sufficient understanding to consider the description along with other information, including information about controls operated by customers themselves. This information serves to obtain an understanding of the customers' information systems, which are relevant for the financial reporting.

Copenhagen, 9 December 2022

Grant Thornton
State Authorised Public Accountants

Jacob Helly Juell-Hansen
State authorised public accountant

Christian H. Riis
Executive director, CISA

Section 4: Control objectives, controls, and service auditor testing

4.1. Purpose and scope

A description and the results of our tests based on the tested controls appear from the tables on the following pages. To the extent that we have identified significant weaknesses in the control environment or deviations therefrom, we have specified this.

This report is issued according to the carve-out method and therefore does not include controls of TimeLog A/S' subservice organisations.

Controls, which are specific to the individual customer solutions, or are performed by TimeLog A/S' customers, are not included in this report.

4.2. Tests

We performed our test of controls at TimeLog A/S, by taking the following actions:

Method	General description
Inquiries	Interview with appropriate personnel at TimeLog A/S regarding controls.
Observation	Observing how controls are performed.
Inspection	Review and evaluation of policies, procedures and documentation concerning the performance of controls. This includes reading and assessment of reports and documents in order to evaluate whether the specific controls are designed in such a way, that they can be expected to be effective when implemented. Further, it is assessed whether controls are monitored and controlled adequately and with suitable intervals.
Re-performance	Re-performance of controls in order to verify that the control is working as assumed.

4.3. Results of tests

Below, we have listed the tests performed by Grant Thornton as basis for the evaluation of the IT general controls with TimeLog A/S.

A.5 Information security policies			
A.5.1 Management direction for information security Control objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
5.1.1	*Policies for information security* A set of policies for information security is defined and approved by management, and then published and communicated to employees and relevant external parties.	We have inspected the information security policy and we have inspected documentation for management approval of the information security policy within the audit period.	No deviations noted.
5.1.2	*Review of policies for information security* The policies for information security are reviewed at planned intervals or if significant changes occur, to ensure their continuing suitability adequacy and effectiveness.	We have inspected, that the information security policy has been reviewed, based on updated risk assessments, to ensure that it still is suitable, adequate, and effective.	No deviations noted.

A.6 Organisation of information security

A.6.1 Internal organisation
Control objective: To establish a management framework to initiate and control the implementation and operation of information security within the organisation

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
6.1.1	*Information security roles and responsibilities* All information security responsibilities are defined and allocated.	We have inspected the organisation chart. We have inspected the guidelines for information security roles and responsibilities.	No deviations noted.
6.1.2	*Segregation of duties* Confliction duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organisations' assets.	We have inspected procedures regarding granting and maintenance of segregation of duties and functions. We have inspected the organisation chart. We have inspected the guidelines for information security roles and responsibilities.	No deviations noted.
6.1.3	*Contact with authorities* Appropriate contacts with relevant authorities are maintained.	We have inspected politics regarding maintenance of regulations concerning contact with relevant authorities.	No deviations noted.

A.6.2 Mobile devices and teleworking Control objective: To ensure the security of teleworking and use of mobile devices			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
6.2.1	*Mobile device policy* Policy and supporting security measures are adopted to manage the risk introduced by using mobile devices.	We have inspected the policy for securing of mobile devices.	No deviations noted.
6.2.2	*Teleworking* Policy and supporting security measures are implemented to protect information accessed, processed and stores at teleworking sites.	We have inspected policy to secure teleworking, and we have inspected the underlaying security measures for protection of remote workspaces.	No deviations noted.

A.7 Human ressource security

A.7.1 Prior to employment Control objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
7.1.1	*Screening* Background verification checks on all candidates for employment is being conducted in accordance with relevant laws regulations and ethics and are proportional to the business requirements the classification of the information to be accessed and the perceived risks.	We have inquired into the procedure for employment of new employees and the security measures needed in the process. We have inspected a selection of contracts with employees in order to determine whether the procedure regarding background check has been followed.	We have observed that in 4 out of 5 samples that it is not evident whether the samples have been screened prior to employment. No further deviations noted.
7.1.2	*Terms and conditions of employment* The contractual agreements with employees and contractors are stating their and the organisation's responsibilities for information security.	We have inspected a selection of contracts with employees and consultants in order to determine whether these are signed by the employees.	No deviations noted.

A.7.2 During employment Control objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities			
No.	**TimeLog A/S' control**	**Grant Thornton's test**	**Test results**
7.2.1	*Management responsibility* Management is requiring all employees and contractors to apply information security in accordance with the established policies and procedures of the organisation.	We have inquired about the procedure for establishing requirements for employees and partners. We have inquired that management has required that employees observe the IT-security policy.	No deviations noted.
7.2.2	*Information security awareness education and training* All employees of the organisation and where relevant contractors, are receiving appropriate awareness education and training and regular updates in organisational policies and procedures as relevant for their job function.	We have inquired about procedures to secure adequate training and education (awareness training). We have inspected documentation for activities, developing and maintaining security awareness with employees.	No deviations noted.
7.2.3	*Disciplinary process* There is a formal and communicated disciplinary process in place, to act against employees who have committed an information security breach.	We have inspected sanctioning guidelines and we have inspected that the guidelines have been communicated.	No deviations noted.

A.7.3 Termination and change of employment Control objective: To protect the organisation's interests as part of the process of changing or terminating employment			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
7.3.1	*Termination or change of employment responsibility* Information security responsibilities and duties that remain valid after termination or change of employment have been defined, communicated to the employee or contractor, and enforced.	We have inquired about employees and contractors' obligation to maintain information security in connection with termination of employment. We have inspected documentation, that information security has been defined and communicated.	We have observed, that in 1 out of 4 samples of employee contracts for terminated employees there is no signature on the employment contract including information security responsibility. No further deviations noted.

A.8 Asset management

A.8.1 Responsibility for assets
Control objective: To identify organisational assets and define appropriate protection responsibilities

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
8.1.1	*Inventory of assets* Assets associated with information and information processing facilities have been identified and an inventory of these assets has been drawn up and maintained.	We have inspected asset listings.	No deviations noted.
8.1.2	*Ownership of assets* Assets maintained in the inventory are being owned.	We have inspected record of asset ownership.	No deviations noted.
8.1.3	*Acceptable use of assets* Rules for the acceptable use of information and of assets associated with information and information processing facilities are being identified, documented, and implemented.	We have inquired about guidelines for the use of assets, and we have inspected the guidelines.	No deviations noted.
8.1.4	*Return of assets* All employees and external party users are returning all the organisational assets in their possession upon termination of their employment contract or agreement.	We have inquired into the procedure for securing the return of assets delivered, and we have inspected the procedure.	No deviations noted.

A.8.3 Media handling Control objective: To prevent unauthorised disclosure, modification, removal, or destruction of information stored on media			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
8.3.2	*Disposal of media* Media are being disposed of securely when no longer required using formal procedures.	We have inquired about media disposal guidelines. We have inspected that media are being disposed of, according to the procedures.	No deviations noted.
8.3.3	*Physical media in transit* Media containing information are protected against unauthorized access misuse or corruption during transportation.	We have inspected procedures for protection of media during transportation.	No deviations noted.

A.9 Access control

A.9.1 Business requirements of access control Control objective: To limit access to information and information processing facilities			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
9.1.1	*Access control policy* An access control policy has been established, documented, and reviewed based on business and information security requirements.	We have inquired into the policy of managing access control in order to establish whether it is updated and approved. We have inspected the access control policy.	No deviations noted.
9.1.2	*Access to network and network services* Users are only being provided with access to the network and network services that they have been specifically authorized to use.	We have inquired about managing access to networks and network services, and we have inspected the solution. We have inspected a number of users, in order to establish that they only have access to approved networks and services, based on work-related requirements.	No deviations noted.

A.9.2 User access management Control objective: To ensure authorised user access and to prevent unauthorised access to systems and services.			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
9.2.1	*User Registration and de-registration* A formal user registration and de-registration process has been implemented to enable assignment of access rights.	We have inquired into the procedure for creating and de-registration of users and we have inspected the procedures. We have inspected a sample of documentation for user creation and removal of users.	No deviations noted.
9.2.2	*User access provisioning* A formal user access provisioning process has been implemented to assign or revoke access rights for all user types to all systems and services.	We have inquired into whether a procedure for user administration has been established. We have inspected that the procedure for user administration has been implemented.	No deviations noted.
9.2.3	*Management of privileged access rights* The allocation and use of privileged access rights have been restricted and controlled.	We have inquired about procedures for granting rights, use and limitation of privileged access rights.	No deviations noted.
9.2.4	*Management of secret authentication information of users* The allocation of secret authentication information is controlled through a formal management process.	We have inquired about procedures for management of secret authentication information of users.	We have observed that there is no formalised procedure for allocation of secret authentication information. No further deviations noted.
9.2.5	*Review of user access rights* Asset owners are reviewing user's access rights at regular intervals	We have inquired into the process of periodic review of users and we have inspected documentation for the review that has been performed during the audit period.	No deviations noted.

No.	TimeLog A/S' control	Grant Thornton's test	Test results
9.2.6	*Removal or adjustment of access rights* Access rights of all employees and external party users to information and information processing facilities are being removed upon termination of their employment contract or agreement or adjusted upon change.	We have inspected procedures about discontinuation and adjustment of access rights. We have, by sample test, inspected resigned employees and we have inspected whether their access rights have been cancelled.	We have observed that in 2 out of 5 samples of removal of access rights, employees have not had their access rights revoked in a timely manner. No further deviations noted.

A.9.3 User responsibilities Control objective: To make users accountable for safeguarding their authentication information			
No.	**TimeLog A/S' control**	**Grant Thornton's test**	**Test results**
9.3.1	*Use of secret authentication information* Users are required to follow the organisation's practices in the use of secret authentication information.	We have inspected the guidelines for the use of secret authentication information.	No deviations noted.

A.9.4 System and application access control Control objective: To prevent unauthorised access to systems and applications			
No.	**TimeLog A/S' control**	**Grant Thornton's test**	**Test results**
9.4.3	*Password management system* Password management systems are interactive and have ensured quality passwords.	We have inspected that policies and procedures require quality passwords. We have inspected that systems for administration of access codes are configured in accordance with the requirements.	No deviations noted.

A.10 Cryptography

A.10.1 Cryptographic controls
Control objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
10.1.1	*Policy on the use of cryptographic controls* A policy for the use of cryptographic controls for protection of information has been developed and implemented.	We have inquired into the policy of using encryption, and we have, by sample test, inspected the use of cryptography.	No deviations noted.
10.1.2	*Key management* A policy on the use protection and lifetime of cryptographic keys has been developed and implemented through their whole lifecycle.	We have inquired into the policies for administering cryptographic keys, supporting the company's use of cryptographic techniques. We have inspected a sample of documentation, in order to establish whether the techniques are used as described.	No deviations noted.

A.12 Operations security

A.12.1 Operational procedures and responsibilities
Control objective: To ensure correct and secure operation of information processing facilities

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
12.1.1	*Documented operating procedures* Operating procedures have been documented and made available to all users.	We have inspected documentation and maintenance of operating procedures. We have inspected that documentation for operating procedures is accessible to relevant employees.	No deviations noted.
12.1.2	*Change management* Changes to the organisation business processes information processing facilities and systems that affect information security have been controlled.	We have inquired about the procedure regarding changes of information handling equipment and -systems. We have inspected a selection of changes, whether they have been documented and implemented in the operation environment, according to the change management procedure and provided in operation reports from vendor.	No deviations noted.
12.1.3	*Capacity management* The use of resources is monitored and adjusted, and future capacity requirements are projected to ensure that the required system performance is obtained.	We have inquired into the procedure for monitoring use of resources and adjustments of capacity, to ensure future capacity requirements. We have inspected that relevant platforms are included in the capacity requirement and included in operations rapports from the sub-supplier.	No deviations noted.
12.1.4	*Separation of development-, test- and operations facilities* Development testing and operational environments are separated to reduce the risks of unauthorized access or changes to the operational environment.	We have inspected how the separation of development-, test- and operations facilities has been established.	No deviations noted.

A 12.2 Protection from malware Control objective: To ensure that information and information processing facilities are protected against malware			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
12.2.1	*Control against malware* Detection prevention and recovery controls to protect against malware have been implemented combined with appropriate user awareness.	We have inquired into measures against malware. We have inquired about the use of antivirus software and we have inspected documentation for its use.	No deviations noted.

A.12.3 Backup Control objective: To protect against loss of data			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
12.3.1	*Information backup* Backup copies of information software and system images are taken and tested regularly in accordance with an agreed backup policy.	We have inquired into configuration of backup and we have inspected samples of documentation for the setup according to the requirements. We have inspected that backup is being monitored. We have inquired about testing of backupfile recovery and we have inspected the documentation for recovery test.	No deviations noted.

A.12.4 Logging and monitoring Control objective: To record events and generate evidence			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
12.4.1	*Event logging* Event logs recording user activities exceptions faults and information security events shall be produced, kept, and regularly reviewed.	We have inquired into logging of user activitues. We have inspected samples of logging configurations.	No deviations noted.

No.	TimeLog A/S' control	Grant Thornton's test	Test results
12.4.2	*Protection of log information* Logging facilities and log information are being protected against tampering and unauthorized access.	We have inquired about secure log information and we have inspected the solution. We have inquired into a selection of logging configurations in order to establish whether login information is protected against manipulation and unauthorized access.	No deviations noted.
12.4.3	*Administrator and operator logs* System administrator and system operator activities have been logged and the logs are protected and regularly reviewed.	We have inquired into procedures regarding logging of activities performed by system administrators and operators. We have inspected logon setups on chosen servers and database systems, in order to establish whether the actions of system administrators and operators are being logged.	No deviations noted.
12.4.4	*Clock synchronization* The clocks of all relevant information processing systems within an organisation or security domain have been synchronised to a single reference time source.	We have inquired into procedures for synchronization against a reassuring time server and we have inspected the solution.	No deviations noted.

A.12.6 Technical vulnerability management Control objective: To prevent exploitation of technical vulnerabilities			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
12.6.1	*Management of technical vulnerabilities* Information about technical vulnerabilities of information systems being used is obtained in a timely fashion, the organisation's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	We have inquired into the procedure regarding gathering and evaluation of technical vulnerabilities. We have, by sample test, inspected servers, database systems and network components in order to establish, whether they are patched in time.	No deviations noted.
12.6.2	*Restriction on software installation* Rules governing the installation of software by users have been established and implemented.	We have inquired into restriction of user executed software installations. We have inspected, that regulations for software installations are being followed.	We have observed that TimeLog does not enforce restriction on software installation. No further deviations noted.

A.13 Communications security

A.13.1 Network security management
Control objective: To ensure the protection of information in networks and its supporting information processing facilities

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
13.1.1	*Network controls* Networks are managed and controlled to protect information in systems and applications.	We have inquired into whether requirements for operating and control of network, including requirements and regulations about encryption, segmentation, firewalls, intrusion detection and other relevant security measures have been defined. We have inspected documentation for network reporting and updating of firewalls.	No deviations noted.
13.1.2	*Security of network services* Security mechanisms service levels and management requirements of all network services are identified and included in network services agreements whether these services are provided in-house or outsourced.	We have inspected reports of network components in order to estimate whether the components have been set up according to requirements and the contractor's recommended baselines.	No deviations noted.
13.1.3	*Segregation of networks* Groups of information services users and information systems are segregated on networks.	We have inquired into the guidelines for segregation of networks. We have inspected a range of accesses made between network zones to establish whether they are limited to essential services.	No deviations noted.

A.13.2 Information transfer Control objective: To maintain the security of information transferred within an organisation and with any external entity			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
13.2.1	*Information transfer policies and procedures* Formal transfer policies procedures and controls are in place to protect the transfer of information using all types of communication facilities.	We have inquired about data transfer policies and procedures and inspected tecnical implementation of encryption of data transfers.	No deviations noted.
13.2.3	*Electronic messaging* Information involved in electronic messaging is appropriately protected.	We have inquired about guidelines for electronic messaging of confidential information.	No deviations noted.
13.2.4	*Confidentiality or non-disclosure agreements* Requirements for confidentiality or non-disclosure agreements reflecting the organisation's needs for the protection of information, are identified, and documented on a regular basis.	We have inquired about the procedure for the establishing of non-disclosure agreements. We have inspected a signed non-disclosure agreement.	No deviations noted.

A.14 Aquisition, development and maintenance of systems

A.14.2 Security, development- and supporting processes
Control objective: To ensure that information security is planned and implemented with the development life cycle

No.	TimeLog A/S' control	Grant Thornton's test	Test results
14.2.1	*Secure development policy* Rules for the development of software and systems have been established and applied to developments within the organisation.	We have inspected the rules for developing software and systems.	No deviations noted.
14.2.2	*Change control procedures* Changes to systems within the development lifecycle are being controlled using formal change control procedures.	We have inquired about the procedure for change management. We have inspected samples of changes, in order to establish whether the change management requirements were met.	No deviations noted.
14.2.3	*Technical review of applications after operating system changes* When operating platforms are changed business critical applications are reviewed and tested to ensure there is no adverse impact on organisational operations or security.	We have inquired into the procedure for technical review of applications after operating system changes.	No deviations noted.
14.2.5	*Secure system engineering process* Principles for engineering secure systems have been established, documented, maintained, and applied to any information system implementation efforts.	We have inspected the procedure for system development.	No deviations noted.
14.2.6	*Secure development environment* There is established appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	We have inspected description of the procedures for establishing a secure development environment. We have inspected, that the procedures have been followed.	No deviations noted.

No.	TimeLog A/S' control	Grant Thornton's test	Test results
14.2.7	*Outsourced development* The organisation is supervising and monitoring the activity of outsourced system development.	We have inspected the procedures for monitoring outsourced development activities.	No deviations noted.
14.2.8	*System security testing* Testing of security functionality is being conducted during development.	We have inquired into whether the system security testing is performed as part of the system development process.	We have observed, that TimeLog does not have guidelines for system security test. No further deviations noted.
14.2.9	*System acceptance testing* Acceptance testing programs and related criteria have been established for new information systems upgrades and new versions.	We have inquired about acceptance testing programs and related criteria for new information systems.	We have observed that TimeLog does not perform system approval tests. No further deviations noted.

A.14.3 Test Data Control objective: To ensure the protection of data used for testing.			
No.	***TimeLog A/S' control***	***Grant Thornton's test***	***Test results***
14.3.1	*Protection of test data* Test data are being carefully selected, protected, managed, and controlled.	We have inspected the procedure regarding selection and protection of test data.	No deviations noted.

A.15 Supplier relationships

15.2 Supplier service delivery management
Control objective: To maintain an agreed level of information security and service delivery in line with supplier agreements

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
15.2.1	*Monitoring and review of third-party services* Organisations are regularly monitoring review and audit supplier service delivery.	We have inquired into whether the procedure for monitoring and review of services from subcontractors is according to the contract. We have inspected a range of status meeting minutes and operations reports, used to ensure that services rendered are according to the contract. Vi have inspected that review and evaluation of relevant audit reports about subcontractors, have been performed.	No deviations noted.
15.2.2	*Manage changes to the third-party services* Changes in supplier services, including maintenance and improvement of existing information security policies, procedures, and controls, are managed under consideration of how critical the business information, systems and processes involved are, and are used for revaluation of risks involved.	We have inquired about management of changes with the subcontractor, and we have inspected documentation for the handling of this.	No deviations noted.

A.16 Information security incident management

A.16.1 Management of information security incidents and improvements
Control objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
16.1.1	*Responsibilities and procedures* Management responsibilities and procedures are established to ensure a quick effective and orderly response to information security incidents.	We have inquired about the responsibilities and procedures of information security incidents, and we have inspected documentation for the distribution of responsibilities. Further, we have inspected the procedure for handling information security incidents.	No deviations noted.
16.1.2	*Reporting information security events* Information security events are being reported through appropriate management channels as quickly as possible.	We have inquired into guidelines for reporting information security incidents and weaknesses, and we have inspected the guidelines.	No deviations noted.
16.1.3	*Reporting security weaknesses* Employees and contractors using the organisation's information systems and services are required to note and report any observed or suspected information security weaknesses in systems or services.	We have inquired about information security events during the period and we have inspected these.	No deviations noted.
16.1.4	*Assessment of and decision on information security events* Information security events are assessed, and it is decided if they are to be classified as information security incidents.	We have inquired into the procedure for assessment, response and evaluation of information security breaches.	No deviations noted.
16.1.5	*Response to information security incidents* Information security incidents are responded to in accordance with the documented procedures.	We have inquired about information security incidents have been responded to, in accordance with the documented procedures.	We have not been able to test the control since no security incidents has occurred during the audit period. No deviations noted.

No.	TimeLog A/S' control	Grant Thornton's test	Test results
16.1.6	*Learning from information security incidents* Knowledge gained from analysing and resolving information security incidents is used to reduce the likelihood or impact of future incidents.	We have inquired about problem management function which analyses information security incidents to reduce the probability of recurrence.	We have not been able to test the control as no security incidents have occurred during the audit period. No deviations noted.

A.17 Information security aspects of business continuity management

A.17.1 Information security continuity
Control objective: Information security continuity should be embedded in the organisation's business continuity management systems

No.	TimeLog A/S' control	Grant Thornton's test	Test results
17.1.1	*Planning information security continuity* Requirements for information security and the continuity of information security management in adverse situations e.g., during a crisis or disaster has been decided upon.	We have inquired into the preparation of a contingency plan to ensure the continuation of operations in the event of crashes and the like, and we have inspected the plan.	No deviations noted.
17.1.2	*Implementing information security continuity* Processes procedures and controls to ensure the required level of continuity for information security during an adverse situation are established, documented, implemented, and maintained.	We have inquired about procedures to ensure that all relevant systems are included in the contingency plan, and we have inspected that the contingency plan is properly maintained.	We have not been able to test the implementation as the test of the contingency plan is scheduled to Q3 2022. No deviations noted.
17.1.3	*Verify review and evaluate information security continuity* The established and implemented information security continuity controls are verified on a regular basis to ensure that they are valid and effective during adverse situations.	We have inquired into testing of the contingency plan, and we have inspected documentation for tests performed.	We have not been able to test the control as the test of the contingency plan is scheduled to Q3 2022. No deviations noted.

A.18 Compliance

A.18.2 Information security reviews
Control objective: To ensure that information security is implemented and operated in accordance with the organisational policies and procedures

No.	*TimeLog A/S' control*	*Grant Thornton's test*	*Test results*
18.2.1	*Independent review of information security* Processes and procedures for information security) (control objectives, controls, policies, processes, and procedures for information security) are reviewed independently at planned intervals or when significant changes occur.	We have observed, that independent evaluation of information security has been established.	No deviations noted.
18.2.2	*Compliance with security policies and standards* Managers are regularly reviewing the compliance of information processing and procedures within their area of responsibility with the appropriate security policies standards and any other security requirements.	We have inquired into management's procedures for compliance with security policies and security standards. We have inspected the annual wheel and the overall governance and compliance, including internal controls.	We have observed a need to strengthen the content of the annual wheel for information security. No further deviations noted.
18.2.3	*Technical compliance review* Information systems are regularly being reviewed for compliance with the organisation' information security policies and standards.	We have inquired for internal controls to ensure compliance with security policies and procedures, and we have inspected selected controls.	No deviations noted.

Section 5: Management's remarks to auditor's test result

Control 7.1.1: TimeLog recognizes the auditor's observation as our documentation is lacking. However, the procedure for screening new employees was in fact carried out. In the future TimeLog will make sure to document procedures accurately.

Control 7.3.1: The personnel folder of one single intern who worked for TimeLog for 6 months was unfortunately deleted. Therefore, it has not been possible to collect documentation of a signed resignation contract. TimeLog will make sure to have necessary backups to avoid equivalent mistakes in the future.

Control 9.3.1: TimeLog recognizes that there currently is no formalized procedure for assigning passwords for secondary systems as TimeLog has for primary systems. Therefore, TimeLog is initiating a documented and formalized procedure as soon as possible.

Control 9.2.6: TimeLog agrees with the observation and will ensure that rights are revoked in immediate connection to the termination of employment. This will be part of our adjusted annual wheel.

Control 12.6.2: TimeLog recognizes the observation and is looking into implementing a hybrid solution to strengthen the control of software installations. Furthermore, TimeLog believes to have mitigated immediate risks by having state of the art antivirus, Microsoft Defender (E5).

Control 14.2.8 and 14.2.9: TimeLog recognizes that there is a mismatch between procedures and documentation. TimeLog has mistakenly placed its work above industry standard expectations. TimeLog believes and always strives to follow general industry standards for security controls, and therefore TimeLog's policies and procedures will be aligned accordingly in the future.

PENNEO

The signatures in this document are legally binding. The document is signed using Penneo™ secure digital signature. The identity of the signers has been recorded, and are listed below.

"By my signature I confirm all dates and content in this document."

Per-Henrik Ole Nielsen
Underskriver 1
Serial number: 22851a76-50bb-4e03-a58b-833ba6bc98e4
IP: 217.63.xxx.xxx
2022-12-12 12:16:10 UTC
MitID

Christian H. Riis
Underskriver 2
Serial number: CVR:34209936-RID:62278486
IP: 5.186.xxx.xxx
2022-12-12 15:05:31 UTC
NEM ID

Jacob Helly Juell-Hansen
Underskriver 3
Serial number: CVR:34209936-RID:50904197
IP: 62.243.xxx.xxx
2022-12-12 21:46:07 UTC
NEM ID