www.pwc.dk

Livehouse

Independent service auditor's ISAE 3402 assurance report on IT general controls as at 26 August 2022 in relation to Livehouse's service to customers

August 2022

pwc

Contents

1 Management's statement

The accompanying description has been prepared for customers who has used Livehouse's services mentioned in section 3 and its auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by customers itself, when assessing the risks of material misstatements in customers financial statements.

Livehouse uses Amazon, Jet-Stream and Hetzner as subservice suppliers for hosting and streaming activities. This report uses the carve-out method and does not comprise controls that Amazon, Jet-Stream and Hetzner performs for Livehouse.

Livehouse confirms that:

a) The accompanying description in section 3 fairly presents Livehouse's services that has processed customers' transactions as at 26 August 2022. The criteria used in making this statement were that the accompanying description:

   (i) Presents how IT general controls in relation to Livehouse's services were designed and implemented, including:

   - The types of services provided
   - The procedures, within both information technology and manual systems, by which the IT general controls were managed
   - Relevant control objectives and controls designed to achieve those objectives
   - Controls that we assumed, in the design of the platform, 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
   - How the system dealt with significant events and conditions other than transactions
   - 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 the IT general controls

   (ii) Includes relevant details of changes to IT general controls in relation to the platform as at 26 August 2022

   (iii) Does not omit or distort information relevant to the scope of the IT general controls in relation to Livehouse's services 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 IT general controls in relation to Livehouse's services that each individual customer may consider important in its own particular environment.

b) The controls related to the control objectives stated in the accompanying description were suitably designed and implemented as at 26 August 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;

Køge, 26 August 2022
Livehouse

Martin Elsborg
CEO

2 Independent service auditor's assurance report on the description and design and implementation of controls

Independent service auditor's ISAE 3402 assurance report on IT general controls as at 26 August 2022 in relation to Livehouse's service to customers

To: Livehouse, customers and customers' auditors

Scope

We have been engaged to provide assurance about Livehouse's description in section 3 of its IT general controls in relation to Livehouse's services which has processed customers' transactions as at 26 August 2022 and about the design related to the control objectives stated in the description.

Livehouse uses Amazon, Jet-Stream and Hetzner as subservice suppliers for hosting and streaming activities. This report uses the carve-out method and does not comprise controls that Amazon, Jet-Stream and Hetzner performs for Livehouse.

We have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon.

Livehouse's responsibilities

Livehouse is responsible for: preparing the description and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the description and statement; providing the services covered by the description; stating the control objectives and designing and implementing controls to achieve the stated control objectives.

Service auditor's independence and quality control

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

PricewaterhouseCoopers is subject to the International Standard on Quality Control (ISQC 1) and accordingly uses and 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.

Service auditor's responsibilities

Our responsibility is to express an opinion on Livehouse's description and on the design and implementation of 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 the International Auditing and Assurance Standards Board, and additional requirements applicable in Denmark. 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 implemented.

An assurance engagement to report on the description and design and implementation of controls at a service organisation involves performing procedures to obtain evidence about the disclosures in the service organisation's description of services and the design and implementation of controls. The procedures selected depend on the service auditor's judgement, including the assessment of risks that the description is not fairly presented, and that controls are not suitably designed or implemented. 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 and described by Livehouse in the Management's statement section.

As mentioned above, we have not performed procedures regarding the operating effectiveness of the controls included in section 4, and therefore we do not express any opinion thereon. 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

Livehouse'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 Livehouse's services that the individual customer may consider important in its particular circumstances. Also, because of their nature, controls at a service organisation may not prevent or detect all errors or omissions in processing or reporting transactions.

Opinion

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

a) The description fairly presents how IT general controls in relation to Livehouse's services were designed and implemented as at 26 August 2022; and

b) The controls related to the control objectives stated in the description were suitably designed implemented as at 26 August 2022.

Description of test of controls

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

Intended users and purpose

This report and the description of tests of controls in section 4 are intended only for customers who have used Livehouse's services and their auditors who have a sufficient understanding to consider it along with other information, including information about controls operated by the customers themselves, in assessing the risks of material misstatement in their financial statements.

Hellerup, 26 August 2022
PricewaterhouseCoopers
Statsautoriseret Revisionspartnerselskab
CVR no. 33 77 12 31

Michael Clement
State-Authorised Public Accountant
mne23410

Mehmet Köse
Senior Manager

3 Description of IT general controls

3.1 Introduction

Livehouse A/S offers an innovative and creative event management platform. This platform can live and host streams virtual and hybrid to the audiences of the customer – as well as branding the events.

3.2 Description of services

Livehouse provides innovative technology -that brings visuals, audio, and video together –and delivers technology-enabled-services that cultivates a coherent and aesthetic experience -enabling customers, colleagues, and business partners to interact closer with one another.

Livehouse's customers arrange events and wishes to broadcast these events. Livehouse supports such events by making available its platform for the livestream. The audience of such events are invited to these events and register to attend.

3.3 Organisation

Key personnel at Livehouse is:

- CEO Martin Elsborg
- Operations Manager Keld Bendtsen
- CTO René Steenfeldt
- Finance Manager Helene Engstrøm
- CXO Lene Jørgensen

3.4 Control environment

Livehouse demonstrates leadership and commitment with respect to the information security management system by:

a) ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organisation;

b) ensuring the integration of the information security management system requirements into the organisation's processes;

c) ensuring that the resources needed for the information security management system are available;

d) communicating the importance of effective information security management and of conforming to the information security management system requirements;

e) ensuring that the information security management system achieves its intended outcome(s);

f) directing and supporting persons to contribute to the effectiveness of the information security management system;

g) promoting continual improvement; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

3.5 Risk management

When planning to implement alterations or additions to the existing platform, the organisation shall consider the needs and expectations of interested parties, and determine the risks and opportunities that need to be addressed to:

To achieve continual improvement of the services, management reviews, evaluates and approves risk assessments according to the implemented annual wheel.

Livehouse's security team shall convene if risks need to be addressed on an hoc basis as per its major incident plans and business continuity plans.

3.6 Information and communication

Livehouse has determined the need for internal and external communications relevant to the information security management system including:

Livehouse shall communicate any suspicion of data breaches upon determination that a breach may have occurred to its customers.

This communication will be made by mail as per contact details provided by the customer.

3.7 Monitoring

Livehouse evaluates the information security performance and the effectiveness of the information security management system.

Livehouse determines:

- A set of controls that are monitored, measured and reported as per the annual wheel.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

Livehouse's use of sub suppliers:

Livehouse uses

- Amazon AWS for hosting and streaming
- Jet-stream Services for streaming (seldomly used, for specific purposes)
- Hetzner Online GmbH for hosting

Amazon is the preferred partner for hosting and streaming, whereas Hetzner is used before production to provide a platform for sharing documents – such as presentations, pictures, logoes to be displayed on screen during production.

3.8 Control objectives and control activities

Livehouse's information security policy is based on the ISO 27001 standard. The following is a description of the control objectives and related control activities considered relevant to IT general controls in relation to the platform providing live streamed virtual and hybrid events.

Control objective CO1 - Governance Management Direction for Information Security

Livehouse has established controls, which ensure that Management has established the required level of information security and procedures to comply with relevant legislation and agreement.

Control objective CO2 - Organisation of information security

Livehouse has established controls ensuring that a management framework initiates and controls the implementation of operation of information security within the organisation.

Control objective CO3 – Human resource security

Livehouse has established controls, which ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.

Control objective CO4 – Asset Management

Livehouse has established controls, which ensures that organizational assets are identified and defined appropriate protection responsibilities

Control objective CO5 – Access Control

Livehouse has established controls, which ensures that access to information and information processing facilities are limited.

Control objective CO6 – Cryptography

Livehouse has established controls, which ensures proper and effective use of cryptography to protect the confidentiality, authenticity and / or integrity of information.

Control objective CO7 – Physical and Environmental Security

Livehouse has established controls, which prevents unauthorized physical access, damage and interference to the organisation's information and information processing facilities.

Control objective CO8 – Operations Security

Livehouse has established controls, which ensures correct and secure operations of information processing facilities.

Control objective CO9 – Communications Security

Livehouse has established controls, which ensures the protection of information in networks and its supporting information processing facilities.

Control objective CO10 – System acquisition, development, and maintenance

Livehouse has established controls, which ensures that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.

Control objective CO11 – Supplier relationships

Livehouse has established controls, which ensures protection of the organisation's assets that is accessible by suppliers.

Control objective CO12 – Information Security Incident Management

Livehouse has established controls, which ensures a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

Control objective CO13 - Information security aspects of business continuity management

Livehouse has established controls, which ensures that information security continuity are embedded in the organisation's business continuity management systems.

Control objective CO14 – Compliance

Livehouse has established controls, which avoids breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.

Section 4 of this document provides a description of the specific control activities for each control objective.

List of omitted control activities, and reasons for omissions

No	Data processor's control activity	Reason
8.3.1	Handling of portable media Procedures have been established for handling portable media	Not applicable
A10	Cryptographie	Provided by supplier
11.1.4	Protection against external and environmental threats Physical protection against adverse effects of fire, flooding, earthquakes, explosions, civil riots and other kinds of natural or man-made disasters have been established and implemented.	Provided by supplier
11.1.6	Public access, delivery and loading areas Access points such as delivery and loading areas and other areas where unauthorised persons can obtain access to the area are controlled and, to the extent possible, separated from information processing equipment to avoid unauthorised access.	Provided by supplier
11.2.1	Placing and protection of equipment Equipment is placed or protected in order to reduce the risk of environmental threats and danger and the risk of unauthorised access.	Provided by supplier
11.2.2	Power supply (back-up power system) Equipment is protected against power failure and other disturbances as a consequence of power supply failure.	Provided by supplier

11.2.3	Protection of cables Cables for electricity and telecommunication transferring data or supporting information services are protected against interference or damage.	Provided by supplier
11.2.4	Maintenance of equipment Equipment is correctly maintained in order to secure its continued accessibility and integrity.	Provided by supplier
12.1.3	Capacity control The use of resources is managed and adjusted, and projections are made of future capacity requirements to ensure that the system is functioning as required.	Provided by supplier
12.2.1	Measures against harmful programs Measures have been taken concerning detection, prevention and recovery in order to protect against harmful code, and adequate procedures have been implemented concerning user awareness.	Provided by supplier
14.2.7	Outsourced development of software The enterprise supervises and monitors outsourced software development. (In case of outsourcing, management and instruction authority follows the assignment to the outsourcing supplier. The purchase of specific development assignments/products is not outsourcing. Offshoring can be either an outsourced assignment or a consultancy assignment).	Not applicable

3.9 Customers' responsibilities

The platform supplied by Livehouse was designed on the assumption that certain controls would be implemented and operated effectively by user organisations.
In certain situations, the application of specific controls of the user organisation is necessary to achieve certain control objectives included in this report.
The list below describes additional controls that should be in operation in user organisations to complement
the controls at Livehouse.

- Controls to ensure that the user organisation validate that input data to Livehouse is correct.
- Controls to ensure that the user organisation act in regard to roles and permissions in case of resignations, retirements or job rotations.

4 Control objectives, control activity, tests and test results

4.1 Purpose and scope

We conducted our engagement in accordance with ISAE 3402, "Assurance Reports on Controls at a Service Organisation", and additional requirements applicable in Denmark.

Our testing of the design and implementation of the controls has included the control objectives and related control activities selected by Management and listed in section 4.3. Any other control objectives, related controls and controls at customers are not covered by our test actions.

We have not performed procedures regarding the operating effectiveness of the controls, and therefore we do not express any opinion thereon.

Our design testing included the control activities deemed necessary to obtain reasonable assurance that the stated control objectives were achieved.

4.2 Test actions

The test actions performed when determining the design and implementation of controls are described below:

Inspection	Reading of documents and reports containing specifications regarding the execution of the control. This includes reading and consideration of reports and other documentation in order to assess whether specific controls are designed so they may be expected to become effective if implemented. We have tested the specific system set-up on the technical platforms and network components in order to verify whether controls are implemented as at 26 August 2022. Among other things, this includes assessment of patching level, password complexity, etc. as well as inspection of equipment and locations.
Inquiries	Inquiry of appropriate personnel. Inquiries have included how the controls are performed.
Observation	We have observed the execution of the control.

4.3 Control objectives, control activity, tests and test results

A5 Security policy					
A5	***5.1***	***Information security policy (Livehouse's IT security policy)*** *Control objective: That Management shows the direction for and supports information security in accordance with business requirements and relevant rules and regulations.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A5	5.1.1	***Written information security policy*** Management approves a written information security policy, which is published and communicated to employees and relevant external parties.	Annually	Observed that an information security policy exists, which has been approved by Management.	No exceptions noted.
A5	5.1.2	***Evaluation of information security policy*** The information security policy is evaluated at planned intervals or in case of significant changes in order to ensure that it is still suitable, complete and efficient.	Annually	Observed that the information security policy has been updated. Inspected the information security policy to ensure that it is complete.	No exceptions noted.

A6 Organisation of information security					
A6	**6.1**	***Internal organisation*** *Control objective: to manage information security in the enterprise.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A6	6.1.1	***Delegation of responsibility for information security*** All responsibility for information security is clearly defined.	Continuously	Inspected documentation showing that the responsibility for information security is clearly defined.	No exceptions noted.
A6	6.1.2	***Segregation of duties*** Functions and areas of responsibility are segregated in order to reduce the risk of unauthorised or unintended change or misappropriation of the enterprise's assets.	Continuously	Inspected guidelines, procedures and organisational structure concerning the allocation and maintenance of segregation of duties and functions. Through inquiries and inspection of system extracts, we checked that system developers do not have access to production environments.	No exceptions noted.

A6 Organisation of information security					
A6	**6.2**	***Mobile devices and teleworking*** *Control objective: to secure information when using mobile equipment and remote workplaces.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A6	6.2.1	***Mobile device policy*** A formal policy has been established, and adequate security measures have been implemented to protect against the risks involved in the use of mobile equipment and communication equipment.	Regularly	Inspected the policy for implementation of security measures for mobile equipment and communication equipment. Inspected that an installation procedure has been implemented for mobile equipment in order to ensure that the set-up of mobile equipment secures confidentiality of data.	No exceptions noted.
A6	6.2.2	***Remote workplaces*** A policy and operational plans and procedures for remote working via mobile workplaces have been prepared and implemented.	Regularly	Inspected policies for remote working via mobile workplaces.	No exceptions noted.

A7 Human resources security					
A7	**7.1**	***Prior to employment*** *Control objective: to ensure that employees, contractors and external users understand their responsibility and are suitable for the assignments for which they are considered, and to reduce the risk of theft, fraud or misuse of facilities.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A7	7.1.1	***Screening*** Verification of job candidates', contractors' and external users' backgrounds is carried out in accordance with relevant laws, regulations and the code of ethics and is aligned with the business requirements, the classification of the information to which access is to be granted, and the relevant risks.	Regularly	Inspected the recruitment procedure and the security-related tasks to be carried out in connection with this procedure. Inspected selected employment contract with a view to ascertaining that the procedure for background checks is complied with in relation to new employees and consultants.	No exceptions noted.
A7	7.1.2	***Terms of employment*** As part of the contractual obligation, employees, contractors and external users sign the terms in the employment contract stating their and the enterprise's responsibility for information security.	Regularly	Inspected procedure ensuring that new employees, contractors and external users confirm to acknowledge their responsibility in relation to professional secrecy by signing the terms. Repeated inspection of selected employment and conclusion of contract in order to check whether employee and third parties had signed and accepted the terms in their employment or supplier's contract.	No exceptions noted.

A7 Human resources security					
A7	**7.2**	***During employment*** *Control objective: to ensure that employees, contractors and external users are aware of security threats and security issues, their responsibilities and duties and that they are able to support the enterprise's security policy when performing their ordinary work, and to reduce the risk of human errors.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A7	7.2.1	***Management's responsibility*** Management requires that employees, contractors and external users maintain security in accordance with the enterprise's established policies and procedures.	Continuously	Inspected descriptions of Management's requirements to employees, contractors and external users. Inspected selected communication from Management to employees pointing out that the security policy must be observed.	No exceptions noted.
A7	7.2.2	***Information security awareness, education and training*** The enterprise's employees and, where relevant, contractors and external users are made aware of security and are regularly kept updated with the enterprise's policies and procedures to the extent this is relevant for their job function.	Regularly	Inspected that attention is drawn to the security policy and other security measures on a regular basis.	No exceptions noted.
A7	7.2.3	***Sanctions*** There is a formal sanction procedure for employees who have committed security breach.	When the incident occurs	Inspected the procedure concerning sanctions against employees, contractors and external users who have committed security breach.	No exceptions noted.

A7 Human resources security					
A7	**7.3**	***Termination or change of employment*** *Control objective: to ensure that termination or change of employees', contractors' and external users' employment takes place in a satisfactory way.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A7	7.3.1	***Cancellation of access rights*** Employees', contractors' and external users' access rights to information and information processing equipment are cancelled when their employment, contract or agreement is terminated, or are adjusted following a change.	Regularly	Inspected the procedure concerning termination of employment and cancellation and adjustment of access rights. Repeated inspection of selected termination of employment in order to check whether the employee's access rights had been cancelled in the access control system.	No exceptions noted.

A8 Asset management					
A8	**8.1**	***Responsibility for assets*** *Control objective: To identify the enterprise's assets and define appropriate protection responsibilities.*			
Item	**Para**	**Control objectives**	**Frequency**	**Tests performed**	**Results of tests**
A8	8.1.1	***Records of assets*** Assets associated with information processing facilities have been identified, and a record of these assets is kept up to date.	Continuously	Inspected that the assets used in relation to Livehouse have been identified and that the record of these assets is kept up to date.	No exceptions noted.
A8	8.1.2	***Ownership of assets*** All information and assets associated with information processing equipment are "owned" by a designated part of the enterprise.	Regularly	Inspected that it is a requirement that all assets have an owner who is responsible for defining and monitoring access requirements and classifications. Inspected selected recorded asset and verified that an owner has been defined.	No exceptions noted.
A8	8.1.3	***Acceptable use of assets*** Rules on the acceptable use of information and assets associated with information processing equipment are identified, documented and implemented.	Regularly	Inspected the procedure for acceptable use of information and assets.	No exceptions noted.
A8	8.1.4	***Return of assets*** All employees, contractors and third-party users are to return all of the enterprise's assets in their possession upon termination of their employment, contract or agreement.	When the incident occurs	Inspected the procedure for termination of employment and the collection of assets. Inquired whether delivered assets are collected.	No exceptions noted.

A8 Asset management					
A8	**8.2**	***Classification of information*** *Control objective: To ensure adequate protection of information proportional to the criticality of the information to the enterprise.*			
Item	**Para**	**Control objectives**	**Frequency**	**Tests performed**	**Results of tests**
A8	8.2.1	***Classification of information*** Information is classified by value, legal requirements, sensitivity and criticality to the enterprise.	Annually	Inspected the procedure for classification of information. Inspected the registration of a selection of essential information assets with a view to ascertaining that the assets are classified.	No exceptions noted.

A8 Asset management					
A8	**8.3**	***Handling of media and customer data*** *Control objective: to prevent unauthorised disclosure, change, removal or destruction of assets and disruption of business activities.*			
Item	**Para**	**Control objectives**	**Frequency**	**Tests performed**	**Results of tests**
A8	8.3.2	***Disposal of media*** When no longer needed, media are safely and properly disposed of in accordance with formal procedures.	When the incident occurs	Inspected the procedure concerning disposal of media. Observed that equipment to be disposed of is stored satisfactorily.	No exceptions noted.

A9 Access control					
A9	**9.1**	***Business requirements to access control*** *Control objective: to control the access to information.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A9	9.1.1	***Policy for access control*** A policy for access control is prepared, documented and evaluated on the basis of business and security-related requirements to access.	Annually	Inspected that a written policy exists for access control, and that this policy is reviewed and updated on a regular basis.	No exceptions noted.
A9	9.1.2	***Access to network and network services*** Users are only granted access to services which they have been specifically authorised to use.	Regularly	Inspected that the procedure for granting users access to services is based on an occupational requirement. Inspected selected user with a view to ascertaining that the user only have access to approved services and that access has been granted on the basis of an occupational requirement.	No exceptions noted.
A9	9.1.6	***Policy for the use of network services*** Users only have access to services which they are specifically authorised to use.	Continuously	Inspected that the procedure concerning allocation of access to services to users is based on an occupational requirement. Observed selected user in order to check that the user only had access to approved services granted based on an occupational requirement.	No exceptions noted.

A9 Access control					
A9	**9.2**	***Administration of user access*** *Control objective: to ensure authorised users' access and to prevent unauthorised access to information systems.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A9	9.2.1	***User registration*** A formal procedure for registration and cancellation of users has been established in respect of allocation and deletion of access to all information systems and services.	When the incident occurs	Inspected procedures concerning allocation and cancellation of access to information systems. Reviewed the process for establishment and cancellation of selected user taking up or leaving their position in order to check whether the procedure for user creation and cancellation has been followed	No exceptions noted.
A9	9.2.2	***Assignment of user access*** Users are only granted access to services which they have been specifically authorised to use.	Regularly	Inspected that the procedure for granting users access to services. Inspected selected user to confirm that the procedure has been implemented in the organisation.	No exceptions noted.
A9	9.2.3	***Administration of privileges*** Allocation and use of privileged rights are limited and controlled.	Continuously	Inspected the allocation of privileged user profiles on selected server in order to assess whether the allocation of privileged rights was based on an occupational requirement.	No exceptions noted.
A9	9.2.4	***Administration of user access codes (passwords)*** The allocation of access codes is controlled by means of a formal administration process.	Regularly	Inspected the procedure concerning control of allocation of access codes.	No exceptions noted.
A9	9.2.5	***Evaluation of user access rights*** Management evaluates the users' access rights at regular intervals by means of a formal process.	Annually	Inspected procedures for regular review and evaluation of access rights. Reviewed the evaluation of user rights for selected user in order to check whether allocated rights reflect an occupational requirement.	No exceptions noted.

A9 Access control					
A9	**9.2**	***Administration of user access*** *Control objective: to ensure authorised users' access and to prevent unauthorised access to information systems.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A9	9.2.6	***Cancellation of access rights*** Employees', contractors' and external users' access rights to information and information processing equipment are cancelled when their employment, contract or agreement is terminated, or are adjusted following a change.	Regularly	Inspected the procedure concerning termination of employment and cancellation and adjustment of access rights. Repeated inspection of selected termination of employment in order to check whether the employee's access rights had been cancelled in the access control system.	No exceptions noted.

A9 Access control					
A9	**9.3**	***User responsibility*** *Control objective: to prevent unauthorised user access and compromising or theft of information and information processing equipment.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A9	9.3.1	***Use of access code*** It is a requirement that the users follow generally accepted security practice when choosing and using access codes.	Continuously	Inspected that requirements to technical implementation of quality requirements in respect of passwords have been described. Inspected that parameters on selected platform support the described requirements to password quality. Inspected selected server in order to check that no users (except system users) are exempted from the technically implemented requirements to passwords.	No exceptions noted.

A9 Access control					
A9	**9.4**	***Management of access to operating systems*** *Control objective: to prevent unauthorised access to operating systems.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A9	9.4.2	***Procedure for safe log-on*** Access to operating systems is controlled by a procedure for safe log-on.	Continuously	Inspected procedures concerning control of access to operating systems. Inspected that user must apply a unique user ID and access code in order to log onto operating systems.	No exceptions noted.
A9	9.4.3	***System for administration of access codes*** Systems for the administration of access codes are interactive and ensure high-quality access codes.	Continuously	Inspected that requirements to high-quality access codes and requirements for password protection are described. Inspected the set-up of technical parameters etc controlling the quality of access codes.	No exceptions noted.
A9	9.4.4	***Use of system tools*** The use of system software that can bypass system and application controls is limited and effectively controlled.	Continuously	Inspected that on selected platform it is only possible for employees with an occupational requirement to use system tools.	No exceptions noted.
A9	9.4.5	***Control of access to software source codes*** Access to software source codes is limited.	Continuously	Inspected procedures concerning limitation of access to software source codes. Inspected a set of source code files in order to check whether access to these was limited to employees with an occupational requirement for access to the source code.	No exceptions noted.

A11 Physical and environmental security					
A11	**11.1**	***Secure areas*** *Control objective: to prevent unauthorised physical access to, damage to and disturbance of the enterprise's premises and information.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A11	11.1.1	***Physical security measures*** Security measures (barriers such as walls, card-controlled entrance gates or manned receptions) are used to protect areas containing information and information processing facilities.	Continuously	Inspected the procedure concerning physical protection of facilities and perimeter security. Inspected relevant premises and perimeter security in order to check whether measures have been taken to prevent unauthorised access.	No exceptions noted.
A11	11.1.2	***Physical access control*** Secure areas are protected by adequate access controls in order to ensure that only authorised staff get access.	Continuously	Inspected the procedure for protection of secure areas. Inspected access point in order to check whether a personal access card is to be used to get access to production facilities.	No exceptions noted.
A11	11.1.3	***Securing of offices*** Physical securing of offices has been established.	Continuously	Inspected that physical securing of offices has been established.	No exceptions noted.

A11 Physical and environmental security					
A11	**11.2**	***Protection of equipment*** *Control objective: to avoid losses, damage, theft or compromising of assets and disruption of the enterprise's activities.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A11	11.2.7	***Secure disposal or reuse of equipment*** All equipment with storage media is controlled to ensure that sensitive data and licence protected software are deleted or securely overwritten before disposal.	Regularly	Inspected the procedure concerning deletion of data on storage media before disposal of the storage medium. Observed test samples of destruction of tapes.	No exceptions noted.
A11	11.2.8	***User equipment without supervision*** The user ensures that equipment without supervision is appropriately protected.	Regularly	Inspected that screen locks have been installed on PCs.	No exceptions noted.

A12 Operations security					
A12	**12.1**	***Operational procedures and areas of responsibility*** *Control objective: to ensure correct and secure operation of information processing equipment.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A12	12.1.1	***Documented operating procedures*** Operating procedures are documented, maintained and made available to users who need them.	Regularly	Inspected selected operational documentation in order to ensure that it had been updated and was accessible to the employees who needed the operating documentation.	No exceptions noted.
A12	12.1.2	***Change management*** Changes to information processing equipment and systems are being controlled.	When the incident occurs	Inspected the procedures concerning changes to information processing equipment and systems. Inspected that a change made to platforms, databases and network equipment had been approved, tested, documented and implemented in the production environment in accordance with the change management procedure.	No exceptions noted.
A12	12.1.4	***Segregation of development, test and operating facilities*** Development, test and operating activities are segregated in order to reduce the risk of unauthorised access or changes to the operating environment.	Continuously	Inspected procedures concerning segregation of development, test and operating environments. Inspected documentation showing that developers only have access to development environments and that only operating staff has access to production environments.	No exceptions noted.

A12 Operations security					
A12	**12.3**	***Back-up*** *Control objective: to maintain integrity and accessibility of information and information processing equipment.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A12	12.3.1	***Information back-up*** Back-ups are made of information and software, and these are tested regularly in accordance with the agreed back-up policy.	Daily	Observed that a back-up policy is described. Inspected procedures concerning back-up of systems and data on the individual platforms. Inspected procedures concerning test of recovery of systems and data from back-ups. Observed that parameters controlling back-ups are maintained. Inspected that regular back-up are made.	No exceptions noted.

A12 Operations security					
A12	**12.4**	***Logging and monitoring*** *Control objective: to disclose unauthorised information processing activities.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A12	12.4.1	***Audit logging (follow-up logging)*** Audit logging to register user activities, exceptions and information security incidents has been performed and is kept for an agreed period in consideration of future investigations and monitoring of access control.	Regularly	Inspected procedures concerning performance and registration of audit logging in connection with user activities, exceptions and information security incidents. Inspected documentation from selected operating system and database in order to check whether audit logging had been activated.	No review of logs has been carried out. However, Livehouse has informed us that they plan to have a log review carried out in December 2022 as part of the annual wheel. No other exceptions noted.
A12	12.4.2	***Protection of log information*** Logging facilities and log information are protected against manipulation and unauthorised access.	Continuously	Inspected selected logging information from platform, network component and database in order to check whether log information is protected against manipulation and unauthorised access.	No exceptions noted.
A12	12.4.3	***Administrator and operator log*** Activities performed by system administrators and operators are logged.	Continuously	Inspected log set-up on selected server in order to check whether system administrators' and operators' activities are logged.	No exceptions noted.
A12	12.4.4	***Time synchronisation*** The clocks in relevant information processing systems in an enterprise or a security domain are synchronised according to an agreed precise time indicating source.	Continuously	Inspected that Network Time Protocol (NTP) has been set up.	No exceptions noted.

A12 Operations security					
A12	**12.5**	***Protection of system files*** *Control objective: to protect system files.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A12	12.5.1	***Control of software on operating systems*** Procedures have been established for control of software installation on operating systems.	Regularly	Inspected procedures concerning software installation on operating systems. Inspected installation and upgrade of selected platform in order to check whether the installation and upgrading are made on a consistent basis in accordance with the procedures.	No exceptions noted.

A12 Operations security					
A12	**12.6**	***Management of technical vulnerabilities*** *Control objective: to reduce risks resulting from utilisation of known technical vulnerabilities.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A12	12.6.1	***Management of technical vulnerabilities*** Information concerning technical vulnerabilities in applied information systems is duly collected; the degree to which the enterprise is exposed to such vulnerabilities is evaluated, and appropriate measures are initiated to handle the related risk.	Regularly	Inspected selected platform in order to check whether it was patched in accordance with the supplier's recommendations.	No penetration test for vulnerabilities of the technical measures has been carried out, just as there is no formalised procedure for the area. However, Livehouse has informed us that they plan to have a penetration test carried out in September 2022 as part of the annual wheel. No other exceptions noted.
A12	12.6.2	***Restrictions on software installation*** Rules on the installation of software have been determined and implemented.		Inspected that the rules on installation of software are implemented. Inspected that the rules on installation of software are complied with.	No exceptions noted.

A13 Communications security					
A13	**13.1**	***Management of network security*** *Control objective: to ensure protection of information in networks and protection of the supporting infrastructure.*			
Item	**Para**	**Control objectives**	**Frequency**	**Tests performed**	**Results of tests**
A13	13.1.1	***Network measures*** Networks are managed and controlled sufficiently to protect them against threats and to maintain the security of the systems and the applications using the network, including transfer of information.	Continuously	Inspected procedures concerning management and control of networks. Inspected selected implemented firewall rules in order to check whether these had been established in accordance with Livehouse's policies as well as recommended baselines from the suppliers.	No exceptions noted.
A13	13.1.2	***Protection of network services*** Security measures, service levels and control requirements to network services are identified and included in an agreement concerning network services, irrespective of whether these services are delivered internally or are outsourced.	Regularly	Inspected that Livehouse's requirements to network security are described in agreements with operating suppliers. Inspected selected firewall rules in order to assess whether the rules established are in accordance with Livehouse's policies as well as recommended baselines from the suppliers.	No exceptions noted.
A13	13.1.3	***Division of network*** Groups of information services, users and information systems are divided in networks.	Continuously	Inspected documentation showing whether the network has been segmented/logically secured in accordance with the network policy.	No exceptions noted.

A13 Communications security					
A13	**13.2**	***Exchange of customer data*** *Control objective: to maintain security in respect of information and software that are exchanged internally in an enterprise and with an external entity.*			
Item	**Para**	**Control objectives**	**Frequency**	**Tests performed**	**Results of tests**
A13	13.2.1	***Policies and procedures for exchange of customer data*** Guidelines, procedures and measures exist in order to protect information exchange in connection with the use of communication equipment.	Continuously	Inspected that communication between Livehouse and customers takes place via encrypted VPN connections.	No exceptions noted.
A13	13.2.2	***Exchange agreements*** Agreements are entered into concerning exchange of information and software between the enterprise and external parties.	When the incident occurs	Inspected selected agreement in order to check whether contract with third parties include a requirement concerning safe exchange of data.	No exceptions noted.
A13	13.2.3	***Electronic information containing customer data*** Customer data in electronic information is protected in a suitable way.	Continuously	Inspected that guideline exist for protection of information in electronic information.	No exceptions noted.
A13	13.2.4	***Confidentiality agreements*** Requirements to agreements concerning confidentiality or secrecy reflecting the enterprise's need to protect information have been identified and are evaluated regularly.	Regularly	Inspected guidelines for confidentiality and secrecy. Inspected selected signed confidentiality agreement in order to check whether the guidelines are observed in connection with employment of new employees and consultants.	No exceptions noted.

A14 System acquisition, development and maintenance					
A14	**14.1**	***Security requirements for information processing systems*** *Control objective: to ensure that security is an integrated part of the information systems.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A14	14.1.1	***Analysis and specification of security requirements*** The business establishes security and control requirements in respect of new information systems or improvement of existing information systems.	Regularly	Inspected the procedure concerning specification of security control requirements in respect of information systems.	No exceptions noted.

A14 System acquisition, development and maintenance					
A14	**14.2**	***Security in development and auxiliary processes*** *Control objective: to maintain security in respect of software and information in business systems.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A14	14.2.2	***Change management procedures*** Implementation of changes is controlled by means of formal change management procedures.	Regularly	Inspected procedures for the management of changes in order to check whether the procedure contains requirements concerning: - Approval - Test - System documentation Inspected selected change in order to check whether the above-mentioned requirements to the management of change were followed.	No exceptions noted.
A14	14.2.3	***Technical review of business systems after changes to operating systems*** In connection with changes to operating systems, business systems critical to the enterprise are evaluated and tested in order to ensure that the change does not have any negative impact on the enterprise's activities and security.	Regularly	Inspected the procedure concerning review of critical business systems as a consequence of changes to the operating system. Inspected selected change in order to check whether tests and review were performed in accordance with the procedure.	No exceptions noted.
A14	14.2.9	***System acceptance*** Criteria have been established for acceptance of new information systems, upgrades and new versions, and suitable testing is made of the system(s) under development and before acceptance of the system(s).	Annually	Inspected guidelines for acceptance of new information systems, upgrades and new versions. Inspected documentation of selected new system, upgrade and change of versions showing that system acceptance has been prepared before the implementation.	No exceptions noted.

A14	14.3	**Test data** *Control objective: To ensure the protection of data used for testing.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A14	14.3.1	***Protection of system test data*** Test data are selected carefully and are protected and controlled.	Regularly	Inspected the procedure concerning selection and protection of test data. Observed a test in order to check whether test data is selected and protected with a view to securing the confidentiality of test data.	No exceptions noted.

A15 Supplier relationships					
	15.1	***External parties*** *Control objective: Maintain security in respect of customer data and information processing equipment to which external parties have access or which is being processed, communicated to or handled by external parties.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A15	15.1.1	***Information security policy for supplier relationships*** The risks to the enterprise's information and information processing equipment from business processes involving external parties are identified, and appropriate controls are implemented before granting access thereto.	When the incident occurs	Inspected the procedure for assessment of third-party suppliers at contract signing. Inspected selected third-party agreement with a view to ascertaining that an assessment of risks in relation to the signing of the contracts was performed.	No exceptions noted.
A15	15.1.2	***Handling of security in agreements with third parties*** Agreements with third parties on access, processing, communication or processing of the enterprise's information or information processing equipment, or whether the procurement of products or services relating to information processing equipment comply with relevant security requirements.	When the incident occurs	Inspected procedure concerning identification of risks and implementation of adequate controls relating to allocating access to the enterprise's information and information processing equipment to external parties.	No exceptions noted.

A15 Supplier relationships					
A15	15.2	***Management of services from third party*** *Control objective: to implement and maintain an adequate level of information security and services in accordance with agreements concerning services from third parties.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A15	15.2.1	***Monitoring and evaluation of services from third parties*** Services, reports and registrations delivered by third parties are currently monitored and evaluated, and audit is performed on a regular basis.	Regularly	Inspected procedures concerning monitoring, review and audit of services provided by third party suppliers. Inspected selected minute of operating meetings and meetings in IT security forum with operating suppliers in order to check whether operating reports received have been reviewed and evaluated and inspected selected operating reports. Inspected that audits have been performed at the most significant operating suppliers.	No exceptions noted.
A15	15.2.2	***Management of changes to services from third parties*** Changes in the procurement of services, including maintenance and improvement of existing information security policies, procedures and measures, are managed considering how critical the business systems and processes involved are and a reassessment of the risks.	Annually	Inspected procedures for changes to delivered services.	No exceptions noted.

A16 Information security incident management					
A16	**16.1**	***Reporting of information security incidents and weaknesses in customer-related systems*** *Control objective: to ensure that information security incidents and weaknesses in connection with information systems are communicated in such a way that corrective action can be initiated in due time.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A16	16.1.1	***Responsibility and procedures*** Management's responsibility and procedures are established in order to ensure quick, effective and systematic handling of information security breaches.	Regularly	Inspected that procedures have been implemented for management's quick, effective and systematic handling of information security breaches.	No exceptions noted.
A16	16.1.2	***Reporting of information security incidents*** Information security incidents are reported through appropriate management channels as quickly as possible.	Regularly	Inspected that procedures have been implemented for registration and reporting of information security incidents. Inspected selected registered security incident in the incident management system in order to check whether adequate analysis is initiated of the reasons, prioritisation and escalation of incident, and that follow-up is made on solutions to the problems. Inspected selected reporting including information on security incidents in the period.	No exceptions noted.
A16	16.1.3	***Reporting of security weaknesses*** Employees, contractors and external users of information systems and services are required to note and report on identified weaknesses or suspected weaknesses in systems and services.	Regularly	Inspected documentation showing that procedures have been implemented for registration and handling of errors etc. Observed that an incident registration system has been implemented in which security incidents can be reported.	No exceptions noted.

A16 Information security incident management					
A16	**16.1**	***Reporting of information security incidents and weaknesses in customer-related systems*** *Control objective: to ensure that information security incidents and weaknesses in connection with information systems are communicated in such a way that corrective action can be initiated in due time.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A16	16.1.4	***Assessment and classification of information security incidents*** Information security incidents are assessed, and it is decided whether they are to be classified as information security breaches.	Regularly	Inspected that security rules contain requirements that security incidents be reviewed regularly. Inspected via random sample that a security incident has been reviewed and assessed.	No exceptions noted.
A16	16.1.5	***Management of information security breaches*** Information security breaches must be handled in accordance with the documented procedures.	When the incident occurs	Inspected that security rules contain requirements that security breaches be handled. Inspected that security breaches are reviewed and assessed in accordance with the implemented procedure.	No exceptions noted.
A16	16.1.6	***Learning from information security breaches*** Mechanisms have been established to quantify and monitor types and scope of information security breaches.	Regularly	Inspected that procedures for quantification and monitoring of types and scope of security incidents have been implemented. Observed that automatic monitoring systems have been implemented which can register and report security incidents in a format that enables reporting of these based on type of incident.	No exceptions noted.

A17 Business continuity management					
A17	**17.1**	***Information security aspects of business continuity management*** *Control objective: to counteract disruption of business activities and to protect critical business processes against the effects of critical information system failure or disaster and to ensure timely recovery.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A17	17.1.1	***Planning information security continuity*** The organisation shall determine its requirements for information security and continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Continuously	Inquired about procedures concerning continuity management and updating of these. Inspected the IT contingency plan in order to ensure that it had been updated.	No exceptions noted.
A17	17.1.2	***Development and implementation of contingency plans, including information security*** Plans have been prepared and implemented for maintaining or re-establishing the enterprise's activities and ensuring accessibility of information at the required level and within the required deadlines after disruption or failure of critical business processes.	Continuously	Inquired whether a contingency plan has been prepared and implemented. Inspected the IT contingency plan in order to check it contains requirements concerning periodic reassessment to ensure that it reflects the need for recovery of IT systems at any time.	No exceptions noted.
A17	17.1.3	***Testing, maintenance and reassessment of contingency plans*** Contingency plans are tested and updated regularly in cooperation with banks and third parties to ensure that they are up-to-date and effective.	Regularly	Inquired about procedures for updating of the contingency plan based on periodic tests of the plan. Inspected the test plan with respect to test of the IT contingency plan, including the result of the test and reporting to Management. Inspected that emergency test have been performed in order to check whether selected decentralised systems, supply lines	No test of the contingency plan has been carried out. However, Livehouse has informed us that they plan to have a test carried out in October 2022 as part of the annual wheel. No other exceptions noted.

A17 Business continuity management					
A17	**17.1**	***Information security aspects of business continuity management*** *Control objective: to counteract disruption of business activities and to protect critical business processes against the effects of critical information system failure or disaster and to ensure timely recovery.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
				and network equipment can be re-established in case of disruption or failure of critical systems.	

A17 Business continuity management					
A17	**17.2**	***Redundancy*** *Control objective: To ensure the availability of information processing facilities.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A17	17.2.1	***Availability of information processing facilities*** Information processing facilities are implemented with redundancy sufficient to meet availability requirements.	Continuously	Inspected that security rules contain requirements that all business-critical systems be redundant.	No exceptions noted.

A18 Compliance					
A18	**18.2**	**Security policies and security standards as well as technical agreement** *Control objective: to ensure that systems comply with the requirements of the enterprise's security policies and security standards.*			
Item	**Para**	**Control objective**	**Frequency**	**Tests performed**	**Results of tests**
A18	18.2.1	***Independent review of information security*** The enterprise's method for managing information security and the implementation thereof (i.e. control objectives, controls, policies, processes and procedures for information security) is reviewed independently and separately at planned intervals or when significant changes occur.	Regularly	Inspected that requirements exist for independent audit reviews of information security. Inspected that an audit of selected important areas inhas been carried out.	No exceptions noted.
A18	18.2.2	***Agreement with security policies and security standards*** Managers ensure that security procedures within their areas of responsibility are correctly complied with in order to obtain agreement with security policies and security standards.	Regularly	Inspected procedures ensuring that managers ensure compliance with security policies and security standards. Inquired whether procedures have been implemented.	No exceptions noted.
A18	18.2.3	***Control of technical agreement*** Information systems are checked regularly with respect to agreement with security implementation standards.	Regularly	Inspected that procedures for periodic control of whether the systems comply with security standards have been implemented for selected network components, platforms and databases.	No exceptions noted.