

Unik System Design A/S

Independent service auditor's ISAE
3402 assurance report on general IT-
controls as of 30 November 2024

The logo for Unik System Design A/S. The word "UNIK" is written in a bold, sans-serif font. The letter "U" is a vibrant blue, while the letters "N", "I", and "K" are a dark purple. The letters are closely spaced and have a slight shadow effect.

Solutions that work for you

Contents

1	Unik System Design's Management Statement	2
2	Independent service auditor's report	4
3	System description	7
4	Control Objectives, control activity, tests and test results	10

1 Unik System Design's Management Statement

The accompanying description has been prepared for customers who have used Unik's SaaS solutions 1) HabiCen for the real estate industry and 2) JustiCase for the legal industry and their auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by subservice organizations and customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Unik System Design uses several subservice organizations accounted for in section 3. Most importantly is GlobalConnect for operations/housing. The Description includes only the control objectives and related controls of Unik System Design and excludes the control objectives and related controls of the subservice organizations. Certain control objectives specified in the Description can be achieved only if subservice organization controls assumed in the design of our controls are suitably designed and implemented. The Description does not extend to controls of the subservice organizations.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls assumed in the design of Unik System Design's controls are suitably designed and implemented, along with related controls at the service organization. The Description does not extend to controls of the customers.

Unik System Design confirms that:

- (a) The accompanying Description in section 3 fairly presents Unik's SaaS solutions HabiCen and JustiCase for processing customers' transactions as at 30 of November 2024. The criteria used in making this statement were that the accompanying Description:
 - (i) Presents how the systems were designed and implemented to process relevant transactions, including, if applicable:
 - The types of services provided, including, as appropriate, classes of transactions processed.
 - The procedures, within both information technology and manual systems, by which those transactions were initiated, recorded, processed, corrected as necessary, and transferred to the reports prepared for customers.
 - The related accounting records, supporting information and specific accounts that were used to initiate, record, process and report transactions; this includes the correction of incorrect information and how information is transferred to the reports prepared for customers.
 - How the system dealt with significant events and conditions, other than transactions.
 - The process used to prepare reports for customers.
 - Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation thereto.
 - Relevant control objectives and controls designed to achieve those objectives.
 - Controls that we assumed, in the design of the system, would be implemented by the customers, and which, if necessary to achieve 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 (including the related business processes) and communication, control activities and monitoring controls that were relevant to processing and reporting customers' transactions.
 - (ii) Does not omit or distort information relevant to the scope of the system being described, while acknowledging that the description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment.

- (b) The controls related to the control objectives stated in the accompanying description were suitably designed as at 30 of November 2024, if controls at subservice organisations were suitably designed and implemented, and customers applied the complementary user entity controls assumed in the design of Unik System Design's controls as at 30 of November 2024. The criteria used in making this statement were that:
- (i) The risks that threatened the achievement of the control objectives stated in the Description were identified; and
 - (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.

Vejle, 19 December 2024
Unik System Design A/S

Jens Find
CEO

2 Independent service auditor's report

Independent service auditors ISAE 3402 assurance report on general IT controls

To: Unik System Design A/S and its customers

Scope

We have been engaged to report on Unik System Design's Description in section 3 of its Unik SaaS solutions 1) HabiCen for the real estate industry and 2) JustiCase for the legal industry for processing customers' transactions as at 30 of November 2024 (the Description), and on the design of controls related to the control objectives stated in the description.

We did not perform any procedures regarding the operating effectiveness of controls included in the Description and, accordingly, do not express an opinion thereon.

The Description indicates that certain control objectives can only be achieved if the complementary user entity controls assumed in the design of Unik System Design's controls are suitably designed and implemented, along with related controls at Unik System Design. Our engagement did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or implementation of such complementary user entity controls.

Unik System Design uses several subservice organizations accounted for in section 3. Most importantly is GlobalConnect for operations/housing. The Description includes only the control objectives and related controls of Unik System Design and excludes the control objectives and related controls of subservice organizations. Certain control objectives specified by Unik System Design can be achieved only if subservice organization controls assumed in the design of Unik System Design's controls are suitably designed and implemented, along with the related controls at Unik System Design. Our engagement did not extend to controls of subservice organizations, and we have not evaluated the suitability of the design or implementation of such subservice organization controls.

Unik System Design's Responsibilities

Unik System Design is responsible for: preparing the Description in section 3 and accompanying statement in section 1, including the completeness, accuracy and method of presentation of the Description and the statement; providing the services covered by the Description; stating the control objectives; identifying the risks that threaten the achievement of the control objectives; selecting the criteria presented in the statement; and designing, implementing and effectively operating controls to achieve the stated control objectives.

Our 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 as well as ethical requirements applicable in Denmark.

EY Godkendt Revisionspartnerselskab applies International Standard on Quality Management 1, ISQM 1, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Our Responsibilities

Our responsibility is to express an opinion on Unik System Design's Description and on the design of controls related to the control objectives stated in that Description, based on our procedures. We conducted our engagement in accordance with International Standard on Assurance Engagements 3402, "Assurance Reports on Controls at a Service Organization," issued by the International Auditing and Assurance Standards Board and additional requirements under Danish audit legislation. That 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.

An assurance engagement to report on the description and design of controls at a service organization involves performing procedures to obtain evidence about the disclosures in the service organization's description of its system, and the design of controls. The procedures selected depend on the service auditor's judgment, including the assessment that the Description is not fairly presented, and that controls are not suitably designed.

An assurance engagement of this type also includes evaluating the overall presentation of the Description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in section 3.

As noted above, we did not perform any procedures regarding the operating effectiveness of controls included in the Description and, accordingly, do not express an 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 Organization

Unik System Design's Description is prepared to meet the common needs of a broad range of customers and their auditors and may not, therefore, include every aspect of the system that each individual customer may consider important in its own particular environment. Also, because of their nature, controls at a service organization 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 report. The criteria we used in forming our opinion are those described in section 1. In our opinion, in all material respects:

- (a) The description fairly presents the Unik's SaaS solutions HabiCen and JustiCase as designed and implemented as at 30 of November 2024; and
- (b) The controls related to the control objectives stated in the Description were suitably designed as at 30 of November 2024, if relevant controls at subservice organisations and complementary controls at customers are suitably designed and implemented as of 30 November 2024, as assumed in the design of Unik System Design's controls.

Description of Tests of Controls

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



Intended Users and Purpose

This report and the description of test of controls in section 4 are intended only for customers who have used HabiCen and JustiCase, and their auditors, who have a sufficient understanding to consider it, along with other information, including information about controls operated by customers themselves, when obtaining an understanding of customers' information systems relevant to financial reporting.

Copenhagen, 19 december 2024
EY Godkendt Revisionspartnerselskab
CVR no.: 30 70 02 28

Jesper D. Sørensen
Partner

Nils B. Christiansen
State Authorized Public Accountant
mne34106

3 System description

3.1 Unik System Design A/S

Unik System Design A/S (Unik) is a Danish-owned company developing and operating software-as-a-service (SaaS) solutions for the property management industry and for the legal sector. Unik's headquarter is located in Vejle, with additional locations in Alborg and Copenhagen. Furthermore, Unik has a team of Polish developers in Warsaw.

3.2 Description of services

The scope of this report is customer's use of Unik's SaaS-solutions HabiCen and JustiCase. The SaaS solutions have the required security level to protect the data stored in the HabiCen and JustiCase solutions. The two solutions continuously synchronize and store data from the on-prem client-server solutions Unik Bolig CE and Unik Advosys CE. Currently, they offer some accounting functionalities, with a few of these functionalities also storing data on the platform.

3.3 System Usage

Customers' system administrative users have access to the SaaS solutions HabiCen and JustiCase for system setup. Customer setup focuses on configuring technical communications' connections, data synchronization and mapping between data models, field types and reporting setup.

End users will still primarily use Unik Bolig CE and Unik Advosys CE, which are set up to synchronize financial transaction data with HabiCen and JustiCase. Users can login to HabiCen and JustiCase to see and create finance reports and file VAT reports. Bookkeeping data will still be created and managed in Unik Bolig CE and Unik Advosys CE. Therefore, regular logging of user access to the solutions has not yet been established.

3.4 Risk Assessment

Risk assessment and management are integrated into Unik's internal processes. Risk management is based on the assessment of technical and organizational risks. Responsibility for risk assessment and management is anchored in the IT security policy with associated internal processes. A compliance department, an information security forum, and a contingency team have been established, sharing responsibility and collaborating on risk management.

Risk assessments are conducted by the system and/or supplier responsible. The risk assessments are based on the likelihood and consequence of identified technical and organizational risks, with a risk rating calculated based on the overall assessment. The risk assessments are reviewed and evaluated by the information security forum. Based on the assessments, an action plan will be initiated if the risk is deemed too high.

3.5 Security measures

The framework for the implemented security measures is ISO 27001/27002 (2022). Security measures and associated control activities have been implemented based on a risk-based approach and are grouped within a range of control objectives. The following describes the controls related to each control objective.

For daily handling and documentation of security controls, including an annual wheel for recurring controls, Unik uses the IT Security Management North GRC from Neupart A/S.

3.6 Control measures

3.6.1 Governance

The framework for information security management is anchored in the IT security policy with associated processes. The IT security policy is approved by the top management. All employees are familiar with the IT security policy and upon hiring employees acknowledge that they have read and understood the IT security policy. Furthermore, all employees sign a confidentiality agreement and confidentiality requirements have been established and agreed upon with external consultants as part of their collaboration with Unik.

The IT security policy includes roles and responsibilities, which are clearly defined and communicated to relevant employees. Furthermore, the IT security policy includes instructions and guidelines for handling IT security and data protection, including procedures for handling information security breaches and incidents.

All employees undergo continuous awareness training for IT security and GDPR, with an onboarding package for review at onboarding and a new awareness course published monthly. Quarterly follow-up is conducted to ensure employees complete the courses.

3.6.2 Technical implementations

Unik maintains registers of relevant assets. Assets are classified and include a description of ownership. The registers are reviewed to ensure that they are up to date.

There are written guidelines for password usage and employees are instructed that passwords are personal and confidential.

Operational procedures for operational activities are in place and are available to all relevant employees. It is secured that all operational procedures are up to date.

Servers are generally protected against malware, with continuous monitoring. Operational systems are continuously maintained with security patches according to an implemented patching strategy. Furthermore, continuous vulnerability scans are performed, which are monitored, and any findings are handled.

Backup procedures have been implemented. Daily backups of data and systems are performed, and backup data is stored separately at two different locations.

Internal network and network in the SaaS solutions are logically segmented to ensure limited access and separation from the public network. This includes separation between development, test and production environments.

In connection with the development of actual functionality in the solutions, procedures for software development have been implemented, including requirements for secure coding principles and system security testing during the development cycle.

Access management and segregation of duties

Access to Unik's systems and databases is secured with secure authentication technologies. Furthermore, privileged rights are being managed and reviewed to ensure that employees only have privileged rights on a work-related basis. Read and write access to source code is restricted to employees with a work-related need.

Segregation of duties is implemented to ensure that access to relevant systems and services are limited to employees with a work-related need. There are written guidelines for granting access and written procedures for registration and deactivation of users. Access to relevant systems and services is reviewed.

3.6.3 Information security in supplier relationships

Supplier management is implemented, which includes that security requirements must be implemented in supplier relationships. The requirements are based on the type of supplier relationship and the services provided.

Risk assessments and classification are based on the criticality of the supplier to secure an adequate level of security. For those suppliers that are critical or important ongoing assessments are made.

Unik uses the following subcontractors in accordance with the delivery of the service regarding the SaaS environment:

Name	Description
Conscensia A/S	Provides consulting services to Unik with a view to developing Unik's solutions. The consultancy services consist of Polish employees, localized in Poland, who work on the same terms as Unik's employees.
GlobalConnect	Supplies and operates the physical infrastructure for the platform from which Unik's SaaS solutions are operated and where the customer's data is stored. Including servers, network, storage system, firewall, internet connection, power supplies, firefighting equipment and cooling.
Unit IT A/S	Stores off-site backup.
Microsoft	Provides a B2C login solution via Microsoft Azure. This solution is used when the customer logs into Unik's SaaS solutions. Only the customer's log-in information is stored.

There are written guidelines for the use of cloud services, and these are communicated to relevant employees.

3.6.4 Management of security incidents

When employees are working remotely security measures are implemented.

All employees are required to report observed or suspected information security incidents to a dedicated department in a timely manner.

All employees must record information security incidents by filling out an incident report.

3.6.5 Physical measures

Physical access safeguards have been implemented to ensure that only authorized personnel are permitted to Unik's premises and data center.

Data bearing medias will be disposed or re-used in a secure way to ensure that data has been removed.

Written guidelines for clear desk rules are implemented and communicated to all employees through the IT security policy.

3.7 Complementary controls at the user entities (customers)

Customers will have the following obligations:

- ▶ to ensure that own users are up to date and are only given to relevant employees
- ▶ to ensure that access conditions meet market standards for secure access, including own users' access to data
- ▶ to assign employees a role that provides different levels of access to the solutions
- ▶ to ensure that personal data stored and recorded in HabiCen and JustiCase are updated
- ▶ to assess the content of free text fields in relation to personal data security (GDPR)

4 Control Objectives, control activity, tests and test results

4.1 Purpose and scope

Our work was performed in accordance with ISAE 3402, Assurance Reports on Controls at a Service Organization.

Our test of the controls' design and implementation comprised the control objective and related controls, which have been selected by Management and which are stated below. Any other control objectives, related controls and controls at customers are not covered by our tests.

The tests performed in connection with the determination of design and operating effectiveness of controls are outlined below.

4.2 Tests performed

Below, we have summarised the tests performed by EY in order to assess controls relevant to Unik System Designs information security and measures.

Inspection	<p>Reading of documents and reports which contain disclosure on the performance of the control. This work includes i.a. the reading of and position-taking to reports and other documentation to assess whether specific controls have been designed in a way that allow them to be effective, if implemented. Furthermore, we assess whether controls are adequately monitored at suitable intervals.</p> <p>As to the technical platforms, databases and network components, we tested the specific system set-up to ensure that controls were designed and implemented as of 30 November 2024. Our tests comprised i.a. an assessment of the patching level, services allowed, segmenting, password complexity, etc.</p>
Inquired	<p>Inquiries of suitable staff with Unik System Design. Inquiries comprised i.a. the performance of controls.</p>
Observation	<p>We observed the performance of controls.</p>

4.3 Control objectives, control activity, tests and test results

Control objective 1: Governance			
Procedures and controls must ensure that management has prepared guidelines for the establishment of information security in accordance with the requirements of the organization as well as relevant laws and regulations.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.1a	<p>Management has approved a written information security policy that has been communicated to all relevant stakeholders, including the employees.</p> <p>Assessments are made on a regular basis - and at least once a year - as to whether the IT security policy should be updated.</p>	<p>Inspected that there is a written information security policy which contains requirements for information security in Unik.</p> <p>Inspected documentation that management has approved the information security policy.</p>	No deviation noted.
5.1b	Upon hiring, employees acknowledge that they have read and understood the information security policy.	Inspected a sample of one, documentation that a newly hired employee has acknowledged having read and understood the information security policy.	No deviation noted.
5.17a	<p>Upon hiring, employees sign a confidentiality agreement.</p> <p>Additionally, the employee is introduced to relevant procedures concerning information security and data processing.</p>	Inspected a sample of one, documentation that a newly hired employee has signed a confidentiality agreement and that the employee was introduced to relevant procedures concerning information security and data processing.	No deviation noted.
5.2	<p>Information security roles and responsibilities are assigned according to Unik's needs and are clearly defined in the Information Security Policy.</p> <p>Information security roles and responsibilities are communicated and assigned to relevant employees</p>	<p>Inspected the information security policy section on organization and responsibility.</p> <p>Inspected documentation for organizational placement of responsibility for information security.</p>	No deviation noted.



Control objective 1: Governance

Procedures and controls must ensure that management has prepared guidelines for the establishment of information security in accordance with the requirements of the organization as well as relevant laws and regulations.

No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.3	Conflicting duties and conflicting areas of responsibility are segregated.	Inspected that formalised procedures are in place for segregating conflicting duties and conflicting areas of responsibility. Inspected that the technical measures agreed support retaining the restriction in users' work-related access to systems.	No deviation noted.
5.4	Management ensures that employees are aware of their information security responsibilities in accordance with Unik's established policies and procedures.	Inspected that the information security policy is available to all employees. Inspected a sample of one, that newly hired employees sign an employment agreement and that information security responsibilities are accounted for herein.	No deviation noted.
5.9a	Assets are identified, and Unik maintains a register of these assets. Ongoing assessments are made - and at least once a year - to determine if the register is up to date.	Inspected inventory of employees' IT assets, as well as inventory of assets in the SaaS environment. Inspected that the register appeared updated.	No deviation noted.
5.9b	The asset register is classified and includes a description of ownership.	Inspected that the list of employees' IT assets, as well as the list of assets used in the SaaS environment, is classified and contains a description of whether the asset is owned by Unik or by the user/employee.	No deviation noted.



Control objective 1: Governance

Procedures and controls must ensure that management has prepared guidelines for the establishment of information security in accordance with the requirements of the organization as well as relevant laws and regulations.

No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.15	There is a written guideline for access control that includes requirements for managing access rights. There are written procedures for registering and deactivating users.	Inspected information security policy. Inspected descriptions of processes for registration and deregistration of users.	No deviation noted.
5.18a	Role-based access has been implemented for Unik's platform, where Unik's SaaS solutions are hosted. Roles are reviewed once a year.	Inspected that role-based access has been implemented for Unik's platform. Inspected a sample of one that documentation exists that user accesses granted are evaluated and authorised on a regular basis - and at least once a year.	No deviation noted.
5.18b	Access to Azure DevOps is re-evaluated once a year ensuring that there is a work-related need for access.	Inspected a sample of one that documentation exists that user accesses granted to Azure DevOps are evaluated and authorised once a year.	No deviation noted.
5.18c	User-accounts are deactivated upon resignation.	Inspected procedures ensuring that resigned or dismissed employees' rights are deactivated or terminated upon resignation or dismissal. Inspected a sample of one documentation that an employee's user access is deactivated upon resignation, close to the assurance date.	No deviation noted.

Control objective 2: Information security in supplier relationships			
Procedures and controls must ensure that information security risks associated with the use of supplier's products or services.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.19a	<p>There are written procedures that include requirements for information security in supplier relationships.</p> <p>A risk assessment and classification are carried out based on the criticality of the suppliers to ensure an adequate level of security.</p>	<p>Inspected written procedures that include requirements for information security in supplier relationships.</p> <p>Inspected a sample of one documentation that a risk assessment has been carried out by a supplier classified as critical.</p>	No deviation noted.
5.19b	<p>Ongoing assessments are made - and at least once a year - to determine if the risk assessments for critical and important suppliers need to be updated.</p>	<p>Inspected that risk assessments for critical and important suppliers have been updated close to the assurance date.</p>	No deviation noted.
5.19c	<p>Confidentiality requirements have been established and agreed upon with external consultants as part of their collaboration with Unik.</p>	<p>Inspected "Non-disclosure agreement" template.</p> <p>Inspected that confidentiality requirements have been established and agreed upon with Consensia as part of their collaboration with Unik.</p>	No deviation noted.
5.20	<p>Information security requirements have been established and agreed upon with IT suppliers based on the type of supplier relationship and the services they provide.</p> <p>Terms and conditions are outlined and contracted in the supplier agreements.</p>	<p>Inspected a sample of one contract with a sub-supplier and related data processing agreement and Service Level Agreement, that information security requirements have been established and agreed upon herein.</p>	No deviation noted.
5.22	<p>Based on a risk assessment, follow-up on individual suppliers is conducted through meetings, inspections, reviews of auditor's reports or similar activity.</p>	<p>Inspected a sample of one, documentation that the auditor's statement for a critical subcontractor has been obtained and reviewed, and that any control deviations have been followed up on.</p>	No deviation noted.



Control objective 2: Information security in supplier relationships

Procedures and controls must ensure that information security risks associated with the use of supplier's products or services.

No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.23	There are written guidelines for the use of cloud services in accordance with Unik's information security requirements. Guidelines and frameworks for the use of cloud services have been communicated to relevant employees.	Inspected guidelines for the use of cloud services. Inspected that guidelines and frameworks for the use of cloud services have been communicated to relevant employees.	No deviation noted.

Control objective 3: Management of security incidents and organisational measures			
Procedures and controls must ensure that organizational security measures are implemented and effective both before and during employment and procedures and controls must ensure that information security incidents are identified and handled.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.24	There are written guidelines for handling information security breaches and incidents, including recording/logging, assessment, reporting, and implementing contingency measures.	Inspected guidelines for handling security incidents, including for registration/logging, assessment and reporting as well as any implementation of preparedness.	No deviations noted.
5.37	Operational procedures for operational activities are documented and made available to all relevant employees. Ongoing assessments are made - and at least once a year - to determine if the procedures need to be updated.	Inspected operating procedures for operational activities. Inspected that operating procedures for operational activities are made available to relevant staff on the Azure DevOps Wiki. Inspected that the procedures are updated around the assurance date.	No deviations noted.
6.3	Mandatory awareness training is provided to all employees on a regular basis. Quarterly follow-ups are conducted to ensure that employees have completed the planned training.	Inspected procedure for awareness training. Inspected a sample of one, that the offered training contains topics within GDPR and information security. Inspected a sample of one, that quarterly follow-up is carried out to ensure that the employees have carried out the planned training.	No deviations noted.
6.8a	All employees are required to report observed or suspected information security incidents to a dedicated department in a timely manner.	Inspected procedure for the handling of information security events. Inspected list of observed or suspected information security events close to the assurance date.	No deviations noted.



Control objective 3: Management of security incidents and organisational measures

Procedures and controls must ensure that organizational security measures are implemented and effective both before and during employment and procedures and controls must ensure that information security incidents are identified and handled.

No.	Unik System Design's control activity	Test performed by EY	Result of EY's test
		Inspected a sample of one, documentation that the information security event was reported to a dedicated department in a timely manner.	
6.8b	All employees must record information security incidents by filling out an incident report.	Inspected procedure for the handling of information security events. Inspected list of observed or suspected information security events close to the assurance date. Inspected a sample of one, documentation that the information security event was recorded by filling out an incident report.	No deviations noted.

Control objective 4: Securing offices, rooms and facilities			
Procedures and controls must ensure only authorized physical access to the organization's information and other associated assets occurs.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
7.3	Based on a risk assessment, physical security has been established to only permit access to facilities and data centre to authorized persons only.	<p>Inspected procedures to ensure that only authorised persons can gain physical access to premises and data centres.</p> <p>Inspected documentation close to the assurance date, that only authorised persons have had physical access to premises and data centres at which personal data are stored and processed, based on a risk assessment.</p>	No deviation noted.
7.7	Unik has implemented a clear desk policy. The policy has been communicated to all employees.	Inspected that Unik has implemented a policy for clear desk and that this has been communicated to all employees.	No deviation noted.
7.14	Items of equipment containing storage media will be disposed or re-used in a secure way to ensure that data has been removed.	Inspected a sample of one, that equipment containing storage media has been disposed or re-used in a secure way to ensure that data has been removed.	No deviation noted.

Control objective 5: Technological controls			
Procedures and controls are complied with to ensure that technical measures to safeguard are implemented.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
5.17b	There are written guidelines for password usage to ensure that all employees follow Unik's practices. Employees are instructed that passwords are personal and confidential.	Inspected written guidelines for password. Inspected password configurations. Inspected that employees are instructed that passwords are personal and confidential.	No deviations noted.
6.7	Security measures are implemented when employees are working remotely.	Inspected that access through a non-approved network requires two-factor authentication. Inspected that access to Unik's domain from outside, requires the establishment of an encrypted VPN connection.	No deviations noted.
8.2	The allocation and use of privileged access rights is restricted and managed. Privileged access rights are reviewed every six months.	Inspected a sample of one employee's privileged access right to Azure DevOps and Unik's SaaS platform, that the user access has a work-related need. Inspected a sample of one, that documentation exists that privileged access rights are evaluated and authorised every six months.	No deviations noted.
8.5	Secure authentication technologies and procedures have been implemented for access control to Unik's SaaS platform.	Inspected documentation that login to Rancher requires the use of multi-factor authentication (MFA) via Azure AD.	No deviations noted.
8.7	Windows servers are protected against malware by an automated tool. The tool is monitored by relevant employees, and any identified incidents will be addressed.	Inspected documentation that Windows servers in the SaaS environment is protected by an anti-malware system. Inspected that any deviations or weaknesses in the technical measures have been addressed.	No deviations noted.

Control objective 5: Technological controls			
Procedures and controls are complied with to ensure that technical measures to safeguard are implemented.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
8.8	Vulnerability scans are performed weekly by an external provider to identify any vulnerabilities. Identified vulnerabilities are evaluated by authorized employees, and appropriate measures are taken.	Inspected for a sample of one, that vulnerability scans are carried out by an external supplier. Inspected for a sample of one, that vulnerabilities identified in the vulnerability scan are evaluated by authorized employees and measures are taken.	No deviations noted.
8.19	Operational systems in Unik's SaaS environment are continuously maintained with relevant updates and patches, including security patches.	Inspected that formalised procedures exist for handling relevant updates and patches, including security patches. Inspected extracts from technical security parameters and setups that systems, databases or networks have been updated using agreed relevant updates, patches and security patches.	No deviations noted.
8.22	Internal networks are logically segmented to ensure restricted access to systems and databases and to separate them from the public network.	Inspected documentation showing whether the network is segmented.	No deviations noted.



Control objective 6: Information backup			
Procedures and controls are complied with to enable recovery from loss of data or systems.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
8.13a	Unik has implemented a written backup strategy and supporting procedures for all servers in the SaaS environment.	Inspected that Unik has implemented a written backup strategy and supporting procedures for all servers in the SaaS environment.	No deviations noted.
8.13b	Backup data is stored and copied to off-site location.	Inspected that backup data is copied and stored to off-site location.	No deviations noted.
8.13c	Backups are performed daily. If a backup job fails, it will automatically be retried within the same backup window. If it fails on the final attempt, a manually follow-up will be performed.	Inspected for a sample of one production server, that the configuration, which ensures that backup job is set to run daily, is activated. Inspected for a sample of one production server, that the backup job is set to restart automatically up to 3 times. Inspected procedure for handling failed backup jobs. Inspected for one sample that the failed backup job was followed up on.	No deviations noted.



Control objective 7: Change management			
Procedures and controls are complied with to preserve information security when executing changes.			
No.	<i>Unik System Design's control activity</i>	<i>Test performed by EY</i>	<i>Result of EY's test</i>
8.4	Read and write access to source code is restricted to employees with a work-related need.	Inspected documentation that read and write access to the Azure DevOps source code is restricted to developers.	No deviations noted.
8.28	Unik has implemented a written procedure for software development that includes requirements for the use of secure coding principles.	Inspected process for developing software for the SaaS environment, including requirements for the use of secure coding principles.	No deviations noted.
8.29	System security tests, including information and personal data security tests, are conducted during the development cycle before applications or code are implemented into the production environment.	Inspected process for developing software for the SaaS environment. Inspected a sample of one, documentation that system security tests, including information and personal data security tests, are conducted during the development cycle before applications or code are implemented into the production environment.	No deviations noted.
8.31	Development, testing and production environments are separated.	Inspected documentation that development, staging and production environments are separated.	No deviations noted.
8.32	Changes to software developed by Unik are managed using formal procedures for change management. The process formally outlines the requirements for the change development cycle.	Inspected process for developing software for the SaaS environment. Inspected for a sample of one, documentation that a development change has followed the change management procedure.	No deviations noted.

PENNEO

Underskrifterne i dette dokument er juridisk bindende. Dokumentet er underskrevet via Penneo™ sikker digital underskrift. Underskrivernes identiteter er blevet registreret, og informationerne er listet herunder.

“Med min underskrift bekræfter jeg indholdet og alle datoer i dette dokument.”

Jens Jensen Find

CEO

På vegne af: Unik System Design A/S

Serienummer: d91ee1b4-c5d4-4873-ac07-b3d53dcce46e

IP: 194.192.xxx.xxx

2024-12-19 15:06:01 UTC



Nils Bonde Christiansen

EY Godkendt Revisionspartnerselskab CVR: 30700228

Statsaut. revisor

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a4c7bea3-5a9f-4f35-bb2c-9ca1124e41f1

IP: 165.225.xxx.xxx

2024-12-19 15:16:24 UTC



Jesper Due Sørensen

EY Godkendt Revisionspartnerselskab CVR: 30700228

Partner

På vegne af: EY Godkendt Revisionspartnerselskab

Serienummer: a6d834d7-442d-428e-ade9-c250dca23ab3

IP: 37.96.xxx.xxx

2024-12-19 15:25:23 UTC



Penneo dokumentnøgle: XBJFF-F3ABV-4YKGS-FOPXP-0TXPI-AQ7EQ

Dette dokument er underskrevet digitalt via **Penneo.com**. Signeringsbeviserne i dokumentet er sikret og valideret ved anvendelse af den matematiske hashværdi af det originale dokument. Dokumentet er låst for ændringer og tidsstempelt med et certifikat fra en betroet tredjepart. Alle kryptografiske signeringsbeviser er indlejret i denne PDF, i tilfælde af de skal anvendes til validering i fremtiden.

Sådan kan du sikre, at dokumentet er originalt

Dette dokument er beskyttet med et Adobe CDS certifikat. Når du åbner dokumentet

i Adobe Reader, kan du se, at dokumentet er certificeret af **Penneo e-signature service <penneo@penneo.com>**. Dette er din garanti for, at indholdet af dokumentet er uændret.

Du har mulighed for at efterprøve de kryptografiske signeringsbeviser indlejret i dokumentet ved at anvende Penneos validator på følgende websted: **https://penneo.com/validator**